TD 92735EN

Installation and Operation Manual
Unite Connectivity Manager

06 March 2013 / Ver. I

About this document

This document is used for the installation and configuration of the product. It is also used for administration, maintenance and troubleshooting. These activities require good knowledge about functionality and limitations, both on module and system level, and also knowledge about how systems, modules and parameters interact.

The document also includes information about the daily operation, that is, creating and sending messages, which can be done by any user in the system.

Cross-references in the document

Throughout this document you will find cross-references in the text which indicate further details that can be found in other sections of this document. The cross-references are colored blue and linked to the relevant place in the document. Positioning your cursor over the cross-reference text and clicking the left mouse button will take you to the relevant section.

To return to the original page after viewing a cross-referred page in Adobe Acrobat or Adobe Reader, click on the ''Previous View'' arrow (or).

Contents

1. Introduction 1
1.1 Licenses for Unite CM 1
1.2 Abbreviation and Glossary 5
1.3 How to Use this Document 6
1.4 Included in the Delivery 8
1.5 Technical Solution 9
1.6 Requirements 9

2 Installation and Configuration steps 10
2.1 Cables and Adapters 10
2.2 Information required for the Setup 10
2.3 Accessing Unite CM 10
2.4 Basic Configuration Steps 11
2.5 Optional Settings 12

3 General 14
3.1 Graphical User Interfaces (GUIs) 14
3.2 Authentication Levels and Default Passwords 16
3.3 Password Settings 17
3.4 Disable the NetBIOS Service 18
3.5 Allow Fragmented TCP Packets 18
3.6 Demonstration Mode 18
3.7 Message Routing Description 19

4 Basic Configuration 20
4.1 Add Users to Unite CM 20
4.2 Additional User Settings 23
4.3 Create Groups 30
4.4 Create User Teams 34
4.5 Create Work Shifts 34
4.6 Import an ESS Backup File 35
4.7 Manage Central Phonebook Entries 38
4.8 Input/Output Setup 39
4.9 Alarm Handling 44
4.10 Basic Alarm Manager 45
4.11 Advanced Event Handling 51
4.12 System Supervision 59
4.13 Status 59
4.14 Module Redundancy 65
4.15 Back up the Configuration 71
4.16 Restore the Configuration 71

4.17 Selection of Data Storage ... 72

5 Device Manager ... 73

6 Device Configuration ... 74

6.1 Device Management Setup ... 74
6.2 Device Handling Configuration ... 75
6.3 Online Status Report Time for Chargers ... 76
6.4 Online Status Report Time for Handsets in a Charging Unit ... 76
6.5 Online Status Report Time for Fixed IP-DECT Devices ... 77
6.6 Service Discovery ... 77

7 Additional System Settings ... 79

7.1 Mail Server Address ... 79
7.2 UNS/User Server ... 79
7.3 Remote Service Center ... 81
7.4 Remote Management ... 82
7.5 Unlock GUI Managed by Unite AM ... 84
7.6 Open Access Protocol (OAP) ... 84
7.7 Java Server/GSM ... 85
7.8 Importing new OA-XML file ... 86
7.9 Logging ... 86
7.10 Time Settings ... 87
7.11 Network Setting ... 88
7.12 Setting License Number for Unite CM ... 89
7.13 Import Smart Device License Document ... 90
7.14 Reboot ... 90

8 Central Phonebook Configuration ... 91

8.1 Technical Specification ... 91
8.2 Customize the Search Result Text ... 91
8.3 Central Phonebook Settings ... 92
8.4 Select Central Phonebook Database ... 93
8.5 LDAP Parameter Setup ... 93
8.6 CMG Parameter Setup ... 95
8.7 Digit manipulation in the Central Phonebook ... 96

9 Serial Interface In ... 100

9.1 Serial Protocol Settings ... 100

10 Serial Interface Out ... 106

10.1 Output Serial Protocol Settings ... 106

11 ASCII Interface ... 109

11.1 Syntax for ASCII Code Translation ... 109
11.2 Data Monitor ... 112

12 Text Displays 114
12.1 Text Display Settings 114
13 SMS via GSM Modem 117
13.1 Add GSM User 117
13.2 Send Message from Unite CM to GSM User 118
13.3 Send SMS from GSM Phone to a Handset in the System 119
14 SMTP Mail Interface 120
14.1 Considerations for Local IT Department 120
14.2 Mail Addressing Options 120
15 DECT Interface 125
15.1 DECT Phone System 125
15.2 Mixed DECT Systems 126
15.3 DECT Interface settings 129
15.4 Absence Handling in DECT 131
15.5 Base Station Conversion 133
16 Cisco Interface 134
16.1 CUCM Configuration 134
16.2 Cisco Interface Configuration 134
16.3 Translations 136
17 WLAN Interface 137
17.1 Handset Registration 137
17.2 Shared Phones 137
17.3 WLAN System 137
17.4 WLAN Message Distribution 138
18 System 900 Interface 139
18.1 System 900 Configuration Page 141
18.2 System 900 Message Distribution 146
19 Create and Send Messages 147
19.1 Create and Send Messages via the Messaging Tool 147
19.2 Create and Send Messages via NetPage 148
19.3 My Groups 150
19.4 Additional Messaging Configuration 150
20 Messaging Administration 156
20.1 Users 156
20.2 Groups 157
20.3 User Teams 159
20.4 Work Shifts 161
20.5 Add Messaging Category 161

20.6 Add S900 Composite Category for Multi-Site Paging ... 162

21 Software Administration ... 164

21.1 Software Information ... 164
21.2 Switch Software ... 164
21.3 Install New Software ... 165

22 Administration of Language and User Interface ... 167

22.1 Customize the Language ... 167
22.2 Customize the User Interface (GUI) ... 170
22.3 Test the New User Interface ... 178
22.4 Update the User Interface after a new Unite CM Release ... 179

23 System Supervision and Security ... 180

23.1 Unite Modules ... 180
23.2 IP Equipment ... 184
23.3 Auxiliary Equipment ... 185
23.4 SNMP Traps ... 188
23.5 Fault Handling ... 191
23.6 Activity Logging ... 197

24 Troubleshooting ... 208

24.1 General Troubleshooting ... 208
24.2 Device Manager Troubleshooting ... 208
24.3 E-mail Interface Troubleshooting ... 209
24.4 Troubleshooting Guide ... 210
24.5 LED Patterns and Troubleshooting Tools in Unite CM ... 220
24.6 Advanced Troubleshooting ... 221
24.7 What to consider when replacing a module ... 221
24.8 Technical Support ... 221

25 Related Documents ... 222

26 Document History ... 223

Appendix A: Used IP Ports ... 227
Appendix B: RS232 Connections ... 228
Appendix C: System 900 Connections ... 232
Appendix D: Network Monitoring in a Redundant System ... 233
Appendix E: Fault Handling Configuration Example ... 235
Appendix F: Alarm Action Configuration Examples ... 238
Appendix G: ASCII-table ... 245
Appendix H: Extracting Information from HL7 v2 Messages ... 246
Appendix I: XML Message Handling in Event Handler ... 253
Appendix J: Protocol Limitations (input) ... 255
Appendix K: Ascom Unite Application Manager ... 258

Appendix L: Services in Unite CM 259
Appendix M: Multiple Event Handlers 261
Index 262

1. Introduction

The Unite Connectivity Manager (Unite CM) is a server software platform used for messaging and alarm handling in your system. It is also used for the administration of users and groups, for supervision, activity logging and fault logging etc. Unite CM is a software on the Elise3 hardware. It can be used independently but also work in combination with other Unite modules or System 900 modules.

An input serial interface is included to enable pagings from external equipment. The input serial interface supports the ESPA 4.4.4 protocol, the Ascom Line protocol and the TAP 1.8 protocol. The Ascom Line protocol is designed to be simple enough to be controlled manually, using a terminal program connected to the serial port.

An output serial interface is also included to support the sending of messages to external paging systems. The output serial interface supports the ESPA 4.4.4 protocol and the TAP 1.8 protocol.

Unite CM is delivered with a basic level of functionality, but depending on customer requests, it can be licensed to have additional levels of functionality.

Messaging features supported by Unite CM include SMS between users in the system, sending instant or predefined text messages from a web browser or messages automatically sent when triggered from for example, a handset or a physical input. It is also possible to send messages to text displays, for example LED signs and corridor displays.

Unite CM also includes a central phonebook which can be accessed from the handsets. The number of entries in the phonebook depends on whether the internal database or an external database is used as phonebook source.

The included Device Manager is used for managing devices such as handsets, desktop chargers and charging racks, that is, handle parameters and software for the devices.

Unite CM can handle different types of protocol and can be used for converting events to actions in your system and it provides an assignment interface to offer the ability for users to dynamically assign recipients to events. It can be used to integrate into Nurse Call systems, Patient Monitoring systems, Laboratory Information systems, Hospital Information systems, Radiology Information systems, Building Management systems, and Security Management systems.

The Unite CM contains a java interface for sending and receiving messages defined by the OA-XML protocol.

Administration of users, groups, user teams, management of alarms from handsets and system units, supervision of other system modules and IP equipment etc. can be done via a remote connection to a customer site.

NOTE: The software uses open-source components and the source code can be downloaded from the website: oss.ascom-ws.com.

1.1 Licenses for Unite CM

1.1.1 Base Licenses

- FE3-C1ALCBAS, Unite Connectivity Manager, Compact BASE
  (Maximum 100 Messaging users).
  The Compact Base license including 10 Messaging users and management of up to 20 devices in Device Management, SMS, Location, Multicast, Broadcast, Remote Management Client, Carrier System Interface[1], Messaging groups, OAP basic one-way

messaging, NetPage, Basic Alarm Manager, Serial input Interface[1] (ESPA, TAP or Ascom Line protocol), System Survey, Supervision, Fault handling, Activity Logging for 1 client.

- FE3-C1ALEBAS, Unite Connectivity Manager, Enterprise BASE
  (Maximum 1000 Messaging users).
  The Enterprise Base license including 10 Messaging users and management of up to 20 devices in Device Management, SMS, Location, Multicast, Broadcast, Basic Web Message Tool, Remote Management Client, Carrier System Interface[1], Messaging groups, OAP basic one-way messaging, System Survey, Supervision, Fault handling, Activity Logging for 1 client.

- FE3-C1ALEEXT, Unite Connectivity Manager, Extension BASE
  The Extension BASE license cannot be used stand-alone. The module must be connected to a Unite CM Compact or Enterprise.
  The Extension Base license including SMS, Location, Multicast, Broadcast, Basic Web Message Tool, Remote Management Client, Carrier System Interface[1], Messaging groups, OAP basic one-way messaging, System Survey, Supervision, Fault handling, Activity Logging for 1 client.

1.1.2 Additional User Licenses

COMPACT BASE

- FE3-C1ALCU10, Unite Connectivity Manager, User license.
  Sold in blocks of 10 users, MoQ[2] = 10 users

Enterprise BASE

- FE3-C1ALEU10, Unite Connectivity Manager, User license.
  Sold in blocks of 10 users, MoQ[3] = 10 users
- FE3-C1ALEUL, Unite Connectivity Manager, User license.
  Sold in blocks of 10 users, MoQ[3] = 50 users
- FE3-C1ALEUC, Unite Connectivity Manager, User license.
  Sold in blocks of 10 users, MoQ[3] = 100 users
- FE3-C1ALEUD, Unite Connectivity Manager, User license.
  Sold in blocks of 10 users, MoQ[3] = 500 users

1.1.3 Other additional Licenses

Compact BASE

- FE3-C1ALCDM, Unite Connectivity Manager, Device Management
  Enables device management for up to 10 000 devices regardless of number of licensed users.
- FE3-C1ALCEC, Unite Connectivity Manager, External Carrier systems interface (ESPA/TAP output interface, GSM modem interface and Text Displays over IP).
- FE3-C1ALCAL, Unite Connectivity Manager, Activity Logging for 30 clients and XML export of Activity Log).

1.The Elise3 Standard module is required for connection to System 900 and RS232 connection to DECT system.
1.Requires Elise3 Standard module
2.Minimum order Quantity

- FE3-C1ALCOAP, Unite Connectivity Manager, Open Access Protocol (OAPv4)
  Basic one-way, Manual Acknowledge, Interactive Messaging (IM), User Data, Alarm, Location, Remote Change of profile, Availability and Poll Location.
- FE3-C1ALCJVM, Unite Connectivity Manager, Java Virtual Machine (JVM)
  Basic one-way, Manual Acknowledge, Interactive Messaging (IM), User Data, Alarm, Location, Remote Change of profile, Availability and Poll Location.
- FE3-C1ALCEH, Unite Connectivity Manager, Advanced Event Handler
- FE3-C1ALCMG, Unite Connectivity Manager, SMTP Mail Interface
- FE3-C1ALCDAC, Unite Connectivity Manager, Duty and Event Assignment Clients
  Number of clients. 1 client (available up to 25 clients).
- FE3-C1ALCAMC, Unite Connectivity Manager, Alarm Management Clients, AMC's
  Number of AMC clients. 1 client (available up to 10 clients).
- FE3-C1ALCL50, Unite Connectivity Manager, Monitor Locations
  Number of Duty & Event Assignment locations. 50 locations (available up to 2 000 locations).
- FE3-C1ALCECG, Unite Connectivity Manager, Cisco External Carrier Gateway (ECG)
- FE3-C2ALCxxx, Unite Connectivity Manager, Module Redundancy

Enterprise BASE / Extension BASE

- FE3-C1ALEDM, Unite Connectivity Manager, Device Management
  Enables device management for up to 10 000 devices regardless of number of licensed users.
- FE3-C1ALENP, Unite Connectivity Manager, NetPage
- FE3-C1ALEBAM, Unite Connectivity Manager, Basic Alarm Manager
- FE3-C1ALESI1, Unite Connectivity Manager, Serial Interface input interface (ESPA, TAP or Ascom Line protocol)
- FE3-C1ALESO, Unite Connectivity Manager, External Carrier systems interface (ESPA/TAP output interface)
- FE3-C1ALEGMI, Unite Connectivity Manager, GSM Modem interface
- FE3-C1ALETD, Unite Connectivity Manager, Text Displays over IP
- FE3-C1ALEAL, Unite Connectivity Manager, Activity Logging for 30 clients and XML export of Activity Log.
- FE3-C1ALEOAP, Unite Connectivity Manager, Open Access Protocol (OAPv4)
- FE3-C1ALEJVM, Unite Connectivity Manager, Java Virtual Machine (JVM)
  Basic one-way, Manual Acknowledge, Interactive Messaging (IM), User Data, Alarm, Location, Remote Change of profile, Availability and Poll Location.
- FE3-C1ALEEH, Unite Connectivity Manager, Advanced Event Handler
- FE3-C1ALEMG, Unite Connectivity Manager, SMTP Mail Interface
- FE3-C1ALEDAC, Unite Connectivity Manager, Duty and Event Assignment Clients
  Number of clients. 1 client (available up to 25 clients).
- FE3-C1ALEAMC, Unite Connectivity Manager, Alarm Management Clients, AMC's
  Number of AMC clients. 1 client (available up to 10 clients).
- FE3-C1ALEL50, Unite Connectivity Manager, Monitor Locations
  Number of Duty & Event Assignment locations. 50 locations (available up to 2000 locations).
- FE3-C1ALEECG, Unite Connectivity Manager, Cisco External Carrier Gateway
- FE3-C2ALExxx, Unite Connectivity Manager, Module Redundancy

For details regarding licenses and technical specifications, refer to the Data Sheet, Unite Connectivity Manager, TD 92739EN.

1.2 Abbreviation and Glossary

A-bus	Serial communication between modules in System 900
Ascom Line protocol	A simple alternative to ESPA 4.4.4 with all basic features of paging call available but with a very limited status report.
CSV	Comma-Separated Values: CSV file format is a file type that stores tabular data. The format dates back to the early days of business computing. For this reason, CSV files are common on all computer platforms.
Category	A system or an application addressed in Unite CM, to send messages to and receive alarms from.
DECT	Digital Enhanced Cordless Telecommunications: global standard for cordless telephony.
ESPA 4.4.4	A message-based serial protocol intended for communication with external equipment. Built upon the ISO1745 transport specification.
Java	Network-oriented programming language.
LAN	Local Area Network: a group of computers and associated devices that share a common communication line.
LDAP[a]	Lightweight Directory Access Protocol
OAJ	Open Access Java: A development kit used for developing customized applications. OAJ is also the service name when addressing the service in Unite addresses.
OA-XML	Open Access protocol used for defining messages in XML format.
SMTP	Simple Mail Transfer Protocol: Global IP protocol used when sending and receiving e-mail.
SNMP	Simple Network Management Protocol: standard for management of network equipment.
System 900	Generic term for teleCOURIER 900.
TAP	Telocator Alphanumeric Protocol: An industry standard protocol for the input of paging request.
TCP	Transmission Control Protocol: Standard IP protocol that enables two hosts to establish connection and exchange streams of data.
teleCARE IP	Ascom's IP based nurse call system.
teleCOURIER 900	Ascom On Site Paging System
Unite	Name of the Ascom IP based system for handling events, messages and alarms
UNS	Unite Name Server: Unite module component that holds the number plan and destinations in Unite.
VoWiFi System	Generic term for Ascom Voice over WiFi System.
WLAN	Wireless Local Area Network

a.LDAP version 3 (LDAPv3) is supported

1.3 How to Use this Document

This sub chapter includes references to other chapters/documents with more detailed information regarding following activities:

1.3.1 Installation and Basic Configuration

- For installation and basic configuration, refer to chapter 2 Installation and Configuration steps on page 10 and chapter 4 Basic Configuration on page 20.

1.3.2 Extended Configuration for additional Compact Licenses

Some extended configuration is included in the Compact BASE license, others require an additional license, see below.

- For settings included in the Unite Connectivity Manager FE3-C1ALCBAS, Compact BASE standard license, see chapters:
  - 4 Basic Configuration on page 20
  - 7.4 Remote Management on page 82
  - 19 Create and Send Messages on page 147
  - 4.9 Alarm Handling on page 44
  - 9 Serial Interface In on page 100
  - 23 System Supervision and Security on page 180
  - 23.6 Activity Logging on page 197 (logging for 1 client at the time)

  (Unite Connectivity Manager FE3-C1ALCU10 license adds users in quantities of 10)

- For settings included in the Unite Connectivity Manager FE3-C1ALCEC, External Carrier systems interface license, see chapters:
  - 10 Serial Interface Out on page 106
  - 13 SMS via GSM Modem on page 117
  - 12 Text Displays on page 114

- For settings included in the Unite Connectivity Manager FE3-C1ALCAL, Activity Logging for 30 clients and XML export of Activity Log, see chapter:
  - 23.6 Activity Logging on page 197 (logging for 30 clients)

- For settings included in the Unite Connectivity Manager FE3-C1ALCOAP, Open Access Protocol (OAPv4), see chapter 7.6 Open Access Protocol (OAP) on page 84.

- For settings included in the Unite Connectivity Manager FE3-C1ALCJVM, Java Virtual Machine (JVM), see chapter 7.7 Java Server/GSM on page 85.

- For settings included in the Unite Connectivity Manager FE3-C1ALCEH, Advanced Event Handler, see chapters:
  - 4.11.2 Action Handler on page 52
  - 11 ASCII Interface on page 109
  - 4.11.3 Event Handler on page 53

- For settings included in the Unite Connectivity Manager FE3-C1ALCMG, SMTP Mail Interface, see chapter 14 SMTP Mail Interface on page 120.

- For settings included in the Unite Connectivity Manager FE3-C1ALCDAC, Duty and Event Assignment Clients, see chapters:
  - 4.11.6 Duty Assignment on page 58 and User Manual, Duty Assignment in Unite Connectivity Manager,
  - 4.11.7 Action Assignment on page 58 and User Manual, Action Assignment in Unite Connectivity Manager

- For settings included in the Unite Connectivity Manager FE3-C1ALCAMC, Alarm Management Clients, AMCs, see chapter 4.11.5 Alarm Management Client (AMC) Management on page 56.

1.3.3 Extended Configuration for additional Enterprise Licenses

Some extended configuration is included in the Enterprise BASE license, other requires an additional license, see below.

- For settings included in the Unite Connectivity Manager FE3-C1ALCBAS, Enterprise BASE standard, see chapters:
  - 4 Basic Configuration on page 20
  - 7.4 Remote Management on page 82
  - 19 Create and Send Messages on page 147 (Messaging Tool only)
  - 23 System Supervision and Security on page 180
  - 23.6 Activity Logging on page 197 (logging for 1 client at the time)

  (Unite Connectivity Manager FE3-C1ALEU10 license adds users in quantities of 10)

- For settings included in the Unite Connectivity Manager FE3-C1ALENP, NetPage license, see chapter 19 Create and Send Messages on page 147.

- For settings included in the Unite Connectivity Manager FE3-C1ALEBAM, Basic Alarm Manager license, see chapter 4.9 Alarm Handling on page 44 (except 4.10.2 Add Locations).

- For settings included in the Unite Connectivity Manager FE3-C1ALEGMI, GSM Modem interface license, see chapter 13 SMS via GSM Modem on page 117.

- For settings included in the Unite Connectivity Manager FE3-C1ALESI1, Serial Interface input interface license, see chapter 9 Serial Interface In on page 100.

- For settings included in the Unite Connectivity Manager FE3-C1ALESO, External Carrier systems interface license, see chapter 10 Serial Interface Out on page 106.

- For settings included in the Unite Connectivity Manager FE3-C1ALETD license, see chapter 12 Text Displays on page 114.

- For settings included in the Unite Connectivity Manager FE3-C1ALEAL, Activity Logging for 30 clients and XML export of Activity Log, see chapter 23.6 Activity Logging on page 197.

- For settings included in the Unite Connectivity Manager FE3-C1ALEOAP, Open Access Protocol (OAPv4), see chapter 7.6 Open Access Protocol (OAP) on page 84.

- For settings included in the Unite Connectivity Manager FE3-C1ALCJVM, Java Virtual Machine (JVM), see chapter 7.7 Java Server/GSM on page 85.

- For settings included in the Unite Connectivity Manager FE3-C1ALEEH, Advanced Event Handler, see chapters:
  - 4.11.2 Action Handler on page 52
  - 11 ASCII Interface on page 109
  - 4.11.3 Event Handler on page 53

- For settings included in the Unite Connectivity Manager FE3-C1ALEMG, SMTP Mail Interface, see chapter 14 SMTP Mail Interface on page 120.

- For settings included in the Unite Connectivity Manager FE3-C1ALEDAC, Duty and Event Assignment Clients, see chapters:
  - 4.11.6 Duty Assignment on page 58
  - 4.11.7 Action Assignment on page 58.

- For settings included in the Unite Connectivity Manager FE3-C1ALEAMC, Alarm Management Clients, AMC's, see chapter 4.11.5 Alarm Management Client (AMC) Management on page 56.

A summary of extended configuration can be found in chapter 2.5 Optional Settings on page 12.

1.3.4 Daily Operation

- For the daily operation i.e. creating and sending messages, refer to chapter 19 Create and Send Messages on page 147.

1.4 Included in the Delivery

- Elise3 hardware including power cable.
  - FE3-C1AAAA & FE3-C1ABAA comes with power plug for EU.
  - FE3-C1AAAB & FE3-C1ABAB comes with power plug for UK, USA & Canada and Australia & New Zealand
- The getting started document; Elise3 – Embedded Linux Server including safety instructions

NOTE: The license certificate must be ordered separately.

1.5 Technical Solution

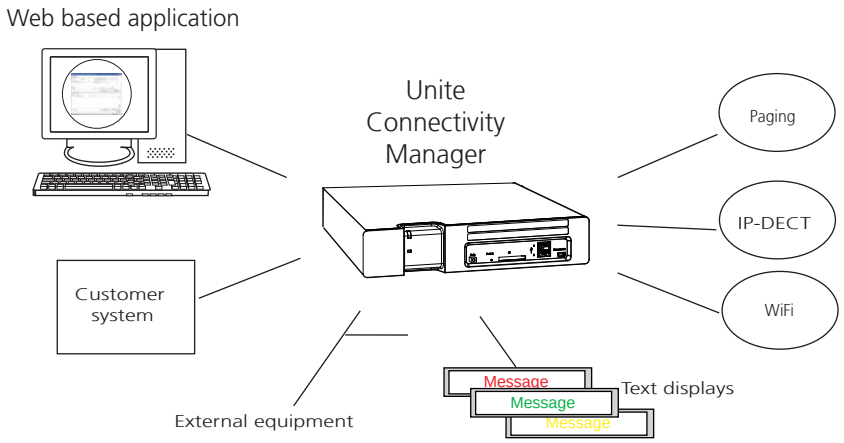


Figure 1. Solution overview

Besides the possibility to connect to Paging system, DECT system and to VoWiFi system, Unite CM can be connected to and receive pagings from external equipment. It can also be connected to and send messages to external text displays.

1.6 Requirements

Refer to the Data Sheet, Unite Connectivity Manager TD 92739EN.

2 Installation and Configuration steps

The installation of Unite CM hardware, that is, Elise3, is described in the Elise3 Installation Guide.

After installing the hardware, the basic configuration is easily done with the help of a setup wizard. The wizard includes all basic settings needed to get Unite CM up and running.

2.1 Cables and Adapters

NOTE: Not included in delivery.

Cables to DECT Exchange and adapters can be ordered separately, refer to the Data Sheet, Unite Connectivity Manager TD 92739EN.

If you want to make your own cable, refer to the descriptions in Appendix B: RS232 Connections on page 228.

2.2 Information required for the Setup

Make sure the following information is available:

- MAC address – found on a label on the Unite CM's rear side, in the application's GUI in the Setup Wizard, or on the Configuration page (the first view).
- License number – found on the license certificate
- Network parameters – ask your network administrator
- Type of connected wireless phone system, if any
- IP address to connected system (if connected via IP)
- Other messaging systems to send messages to (optional)
- IP address to mail server if fault information and Activity Logs are to be sent to e-mail recipients (optional)
- LDAP[1] properties if an LDAP server is used as Central Phonebook directory (optional)

2.3 Accessing Unite CM

2.3.1 Getting Started

When accessing Unite CM for the first time, follow the instructions in the Elise3 – Embedded Linux Server including safety instructions M0275130 (enclosed in the delivery) or the Installation Guide, Elise3, TD 92679GB.

NOTE: The IP address must not change during operation because renew of IP address via DHCP is not handled. Other equipment connected to this product also expects a fixed IP address in some cases. If the IP plan is changed, this product must be restarted to update the IP address. Otherwise the system will not function properly.

1.LDAP version 3 (LDAPv3) is supported

2.4 Basic Configuration Steps

Figure 2. The Setup Wizard

The first time and as long as Unite CM is not configured, the setup wizard will start automatically when logging on from a web browser. It requires an ''admin'' or ''sysadmin'' password, refer to 3 General on page 14.

The content of the wizard is depending on the license. It means that all configuration is not shown for all licenses.

1 Log on to Unite CM.

The setup wizard will open and help you with the basic configuration. The setup wizard includes the following settings:

- Network setup – can be set manually or via DHCP.
- License number – the type of license determines the functionality. The license number is mapped to a specific module key. The module key is shown in the Wizard.
- Type of connected wireless phone system – the exchange used by the handsets in the system. Select ''None'' for handsets in the VoWiFi System.
- IP address to the connected DECT phone system (if connected via IP).
- Serial Interface (input) – enables paging from external equipment (using ESPA, Ascom Line protocol or TAP).
- Description of connected messaging systems – i.e. systems Unite CM should be able to send text messages to and receive personal alarms from. The description is used when setting up users with messaging handsets. Use a description, max 50 characters long, that is familiar to the persons administering the users.
- Address to the mail server – to be able to send fault information and export activity logs via e-mail.
- Date and time properties/settings – for time stamps on activities.
- Phonebook properties – database to use when searching (local phonebook on Unite CM, LDAP server or CMG server).
- LDAP/CMG Properties – (only visible if LDAP/CMG is selected in the Central Phonebook Properties)
- Passwords – change from default to site specific passwords.

2 Add users.

To enable messaging to and between handsets, all users must be added to Unite CM. Refer to 4.1 Add Users to Unite CM on page 20.

3 Create groups (optional).

Groups makes it possible to send one message to several handsets. Refer to 4.3 Create Groups on page 30.

4 Create User Teams (optional).

User Teams makes it possible to give users different access rights. Refer to 4.4 Create User Teams on page 34. Access rights for User Teams needs to be defined if Duty Assignment is going to be used.

5 Create work shifts (optional).

Work shifts makes it possible to create diversions to different Call IDs depending on active work shift. Refer to 4.5 Create Work Shifts on page 34.

6 Create an individual password for logging in to the system (optional).

Refer to 4.2 Additional User Settings on page 23.

7 Configure the phonebook if the local database is used (when not using LDAP/CMG server), refer to 4.7 Manage Central Phonebook Entries on page 38.

8 Create a security backup.

We recommend you to create a security backup of all settings (to facilitate the configuration in case of a system failure). Refer to 4.15 Back up the Configuration on page 71.

2.5 Optional Settings

Some of the optional settings in Unite CM are included in the basic license, others require an additional license, refer to 1.3 How to Use this Document on page 6.

- Alarm Handling – alarm actions can be set (type of trigger and what action to take). Refer to chapter 4.9 Alarm Handling on page 44 and 4.11 Advanced Event Handling on page 51.
- Fault Handling – actions on an incoming fault can be set. Possible actions are output activation, sending a message, sending a fault notification via SNMP Trap or via E-mail. The actions start depending on trigger conditions. Refer to chapter 23.5 Fault Handling on page 191.
- Survey System – other Unite modules in the system can be surveyed. Refer to chapter 23.1.1 System Survey on page 180.
- Supervision – makes it possible to supervise the system. Refer to chapter 23 System Supervision and Security on page 180.
- Activity Logging – incoming activities can be filtered and stored. The logs can be manually and automatically exported for future analysis. Refer to chapter 23.6 Activity Logging on page 197.
- Status – information about the site and information about supervised modules and equipment can be exported for troubleshooting purposes. Refer to chapter 4.13 Status on page 59.
- Set Language – the user interface language can be translated, refer to chapter 22.1 Customize the Language on page 167.
- Input/Output setup – makes it possible to define inputs (for example a switch or button) and outputs (for example to turn on a siren or to close a door). Inputs can be used as trigger conditions and outputs can be used as actions. Refer to chapter 4.8 Input/Output Setup on page 39.
- Customize the Start page and NetPage GUI – the Start page and the NetPage user interface can be customized to suit the individual customer requirements concerning functionality. Refer to chapter 22.2 Customize the User Interface (GUI) on page 170.
- Remote Connection – it is possible to establish a remote connection to a customer site which makes it possible to configure and maintain sites, independent of distance. Refer to chapter 7.4 Remote Management on page 82.
- Open Access Protocol (OAP) – enables communication with other systems connected to Unite CM. Refer to chapter 7.6 Open Access Protocol (OAP) on page 84.
- Java Server – makes it possible to develop customized applications for communication with other systems connected to Unite CM. Refer to chapter 7.7 Java Server/GSM on page 85.

- SMTP Mail – makes it possible to receive/send SMTP mail. Refer to chapter 14 SMTP Mail Interface on page 120.
- Module Redundancy – makes it possible to set up a pair of Unite CM modules for redundancy. Refer to chapter Module Redundancy on page 65.
- Cisco Interface - makes is possible to establish a connection between the Unite CM and Cisco IP phones. Refer to chapter Cisco Interface Configuration on page 134.

3 General

3.1 Graphical User Interfaces (GUIs)

3.1.1 Start Page

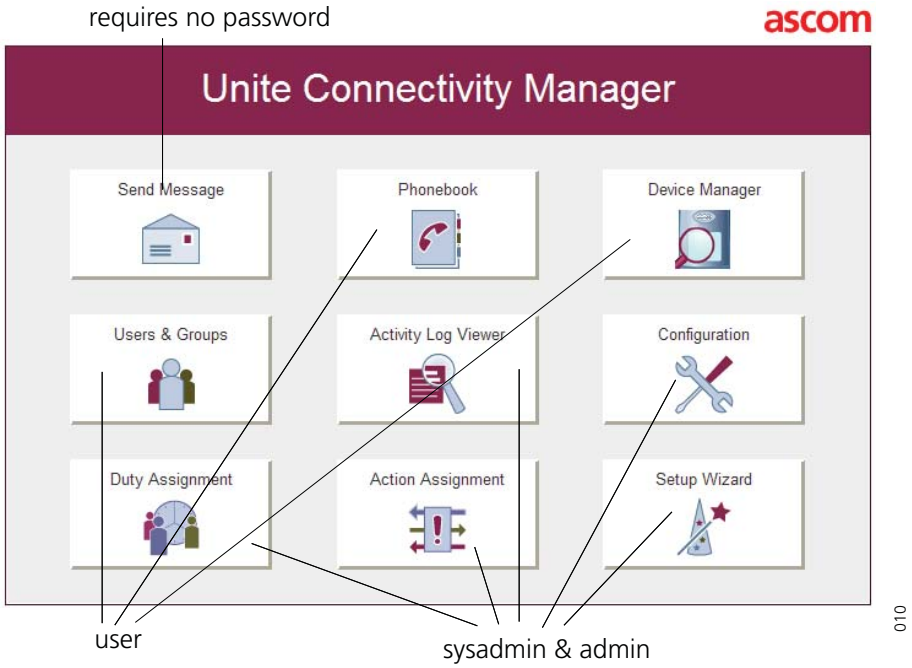


Figure 3. Unite CM start page

The start page has entrances to different applications. The number and type of applications is license dependent. Different applications also requires different authentication levels as shown in the illustration above, see Authentication Levels and Default Passwords on page 16.

3.1.2 Configuration Page

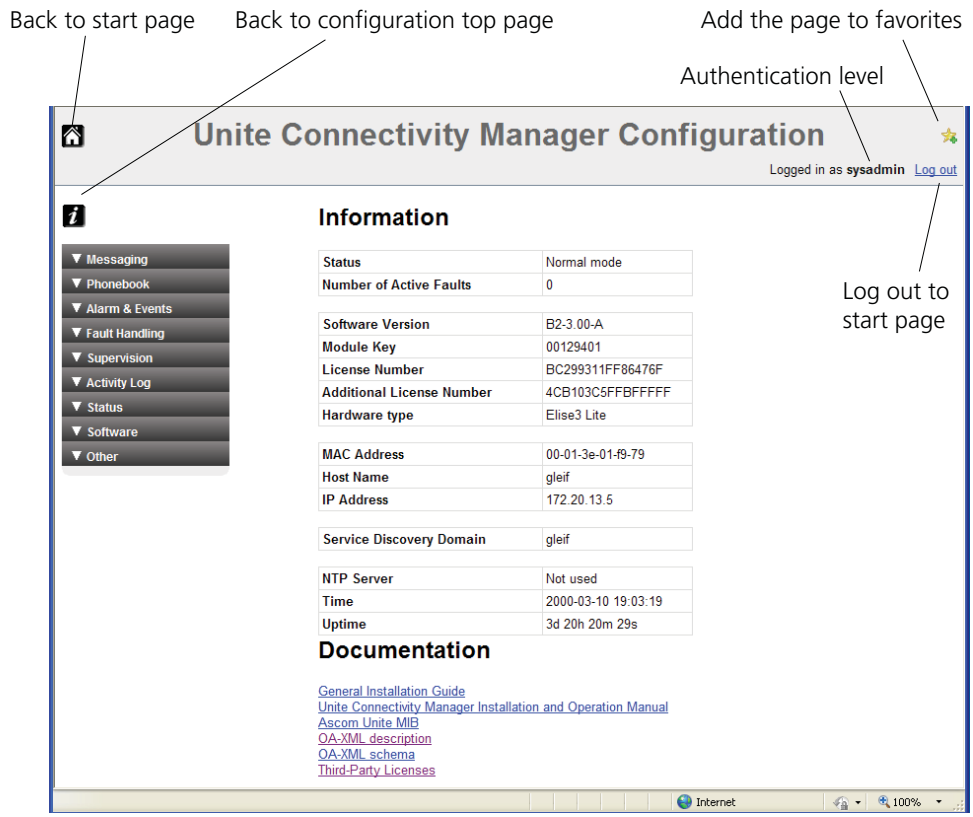


Figure 4. The Configuration page

With system administrator or administrator rights you will be able to access the complete Unite CM configuration page from the Configuration-, Phonebook- and Users & Groups buttons on the start page. Links to documentation are also found on the configuration page.

Use the symbol if you want to return to the start page without logging out. Using the ''Log out'' link will also send you back to the start page but you will be logged out as well.

System information is shown on the Configuration top page, for example host name, IP address and MAC Address.

3.1.3 Advanced Configuration page

The Advanced Configuration page is reached from the Configuration page (under Other).

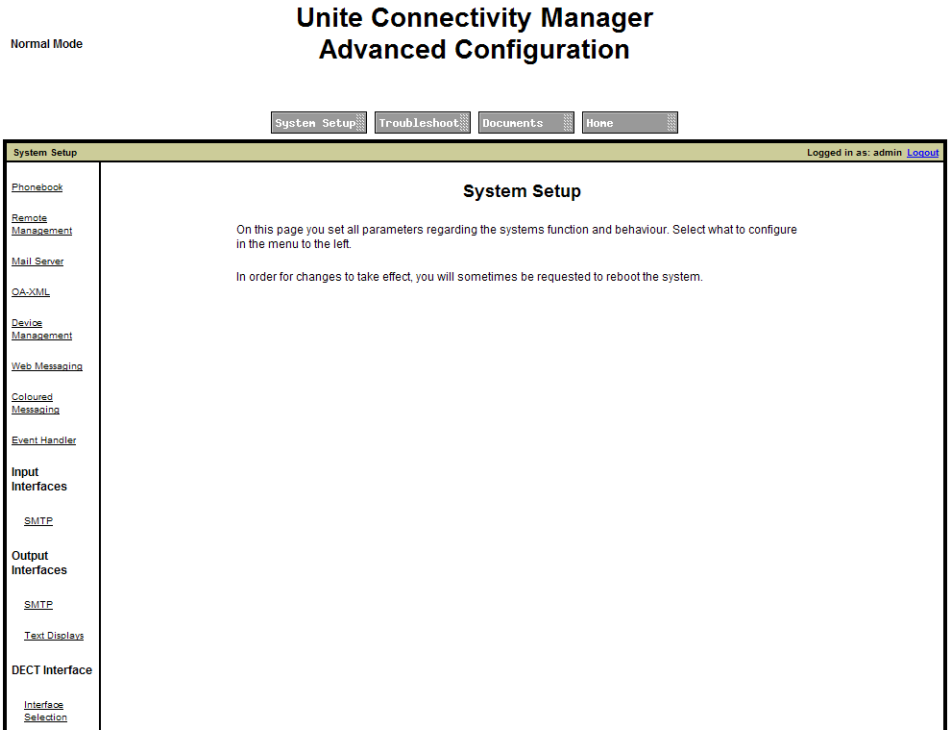


Figure 5. The Advanced Configuration page

3.2 Authentication Levels and Default Passwords

Unite CM has different authentication levels:

- Using the Send Message function, i.e. creating and sending messages can be done by any user in the system and requires normally no password, but individual passwords for logging in to the system can be created.
- User rights are required for the administration of users & groups and the phonebook. Default user name and password are ''user'' and ''password''.
- Administrator rights are required for the setup, the configuration and administration of Unite CM, simple troubleshooting and changing passwords (except for the sysadmin password). Default user name and password are ''admin'' and ''changeme''.
- System Administrator rights are used for advanced troubleshooting, gives access to all administration pages and the permission to change all passwords. Default user name and password are ''sysadmin'' and ''setmeup''.

Functionality matrix

The following matrix shows which functionality that can be used by the different authentication levels.

	anonymous	user	admin	sysadmin
Send messages	Yes	Yes	Yes	Yes
Phonebook administration NetPage login	No	Yes	Yes	Yes
View configuration settings	No	No	Yes	Yes

Unite CM configuration Access to the setup wizard	No	No	Yes	Yes
Change passwords	No	No	Yes[a]	Yes

a.admin cannot change password for sysadmin.

3.3 Password Settings

The default passwords for the different type of users; sysadmin, admin etc., can be changed and it is also possible to specify the password complexity, such as length and number of character types. Passwords can be changed in both the Setup Wizard and on the *Advanced Configuration* page, but the password complexity (password policy) can only be changed on the *Advanced Configuration* page.

It is possible to change passwords for different users in both the Setup Wizard and from the Advanced Configuration page.

3.3.1 Change Passwords

1 Click ''Configuration'' on the start page.

2 Select Other > Advanced Configuration in the menu on the *Configuration* page.

3 Click ''Change Passwords'' under Security in the menu on the *Advanced Configuration* page.

4 Select the user you want to change password for.

5 Enter your user name and password. Enter the new password and confirm the password.

6 Click ''Ch. Passwd''.

3.3.2 Set Password Policy

The required password complexity can be set.

1 Click ''Configuration'' on the start page.

2 Select Other > Advanced Configuration in the menu in the on the *Configuration* page.

3 Select ''Password policy'' under Security in the menu on the *Advanced Configuration* page.

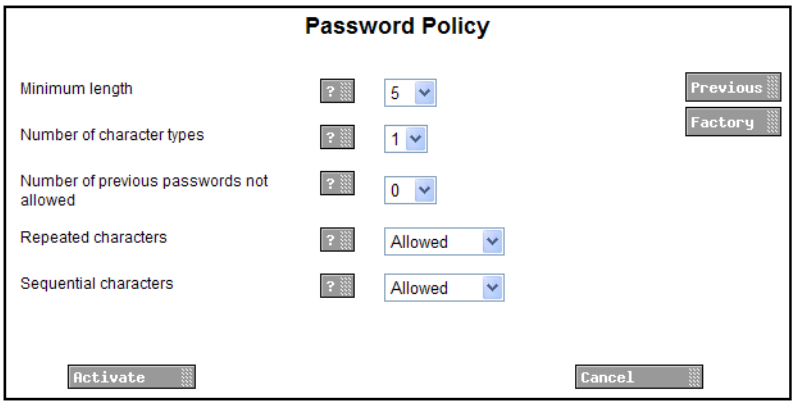


Figure 6. The Password Policy page

4 Select password policy.

5 Click ''Activate''.

It is also possible to select previous or factory default settings.

Security settings, such as not allowing HTTP and FTP access, disabling NETBIOS and increasing the security by using Certificates might be needed if required by the customer.

3.4 Disable the NetBIOS Service

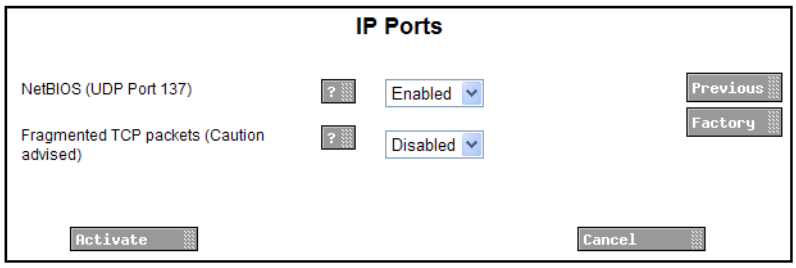
Security settings, such as disabling NETBIOS might be needed if required by the customer. The NetBIOS port is default enabled but can be disabled if needed for security reasons.

The NETBIOS Service makes it possible to access the module with the NetBIOS name ''elise-XXXXXXXX'', where XXXXXXXX is the module key number.

1 Click ''Configuration'' on the start page.

2 Select Other Settings > Advanced Configuration in the menu on the *Configuration* page.

3 Select ''IP Ports'' under Security in the menu on the *Advanced Configuration* page.



4 Select ''Disabled'' in the *NetBIOS (UDP Port 137)* drop down list.

5 Click ''Activate''.

3.5 Allow Fragmented TCP Packets

Fragmenting is when the IP protocol allows an IP packet to be broken apart into several smaller packets, which then can be transmitted and reassembled at the final destination.

If the network has a MTU value lower than the default 1500 bytes, packets will be dropped if not fragmenting is allowed. If fragmentation is allowed in the network the parameter needs to be enabled in Unite CM.

1 Click ''Configuration'' on the start page.

2 Select Other Settings > Advanced Configuration in the menu on the *Configuration* page.

3 Select ''IP Ports'' under Security in the menu on the *Advanced Configuration* page.

4 Select ''Enabled'' in the *Fragmented TCP packets (Caution advised)* drop down list.

5 Click ''Activate''.

3.6 Demonstration Mode

Demonstration Mode makes it possible to run Unite CM for two hours with almost full functionality of the application.

Limitations: In Device Management, File Download and Baseline will be deactivated.

The Demonstration Mode can be set from the application's Configuration page or manually by using the Mode button. The module will automatically return to previous license and parameters (without restart) after 2 hours.

Demonstration Mode is indicated by the Status LED with yellow slow flashing light. If any application encounters problems during Demonstration Mode, the Status LED will however show red slow flashing light instead. The Mode button LED shows blue fixed light.

From the application's Configuration page:

1 Click ''Configuration'' on the start page.

2 Select Other > Demonstration Mode in the menu on the *Configuration* page.

3 Click ''Activate''.

4 Exiting before the 2 hours have passed, is done by clicking ''Deactivate''.

Using the Mode button:

1 Press and hold the Mode button for 10 seconds.

3.7 Message Routing Description

The UNS supports message routing consisting of a set of rules that make it possible to do the following:

- Divert a message to other systems/users when for example the origin user is absent or out of range. A user can have more than one diversion condition connected to the Call ID. This makes it possible for the user to be reached in many systems and minimizes the risk of losing a message when being out of range in one system. See 4.2 Additional User Settings on page 23 for configuration example and also Function Description, Number Planning and Message Routing in Unite, TD 92254GB.
- Forward a message to a user located in another number plan/site if his/her Call ID is not found in the local number plan. See 7.2 UNS/User Server on page 79 and also Function Description, Number Planning and Message Routing in Unite, TD 92254GB.

Number Plan in UNS

The number plan translates Call IDs to Unite destination addresses. Every Call ID corresponds to a Number/Address (for example a handset's call number or an e-mail address) to which a message is sent. In the Number Plan, all Call IDs must be defined. A Call ID can either be numerical or a text string.

The following list gives an example of a number planning table (the destination address format is written as Number/Address -> Category where category stands for an IP address with a service, for example Number/Address -> 172.23.9.151/DECT).

Call ID	Destination Address
7123	9123 -> DECT phone
8123	9123 -> Pager
Lars	9401 -> DECT phone

4 Basic Configuration

The basic configuration requires system administrator or administrator rights. With user rights you will only be able to access and configure Users & Groups and the Phonebook. Refer to chapter 3 General on page 14.

4.1 Add Users to Unite CM

There are several ways to add users to the Unite CM:

- Add users manually
- Import users from a CSV file, 4.1.3 Import users from a CSV file on page 22
- Import messaging configuration from an ESS backup file, see 4.6 Import an ESS Backup File on page 35

Depending on how the users are added, additional configuration might be set as shown in the table below:

	Manually	CSV file	ESS backup file
Users	x	x	x
Messaging categories	-	-	x
Groups	-	-	x
Work shifts	-	-	x
Teams	-	-	x
Diversions	-	-	-

4.1.1 Add users manually

Users must be added to enable messaging in the system and any User Team and/or Work Shift the user shall belong to, must be defined before a user can be added to it. Refer to 4.4 Create User Teams on page 34 and 4.5 Create Work Shifts on page 34. The messaging system to which the user belongs, that is, Category, is defined in the Setup Wizard.

Figure 7. Users & Groups

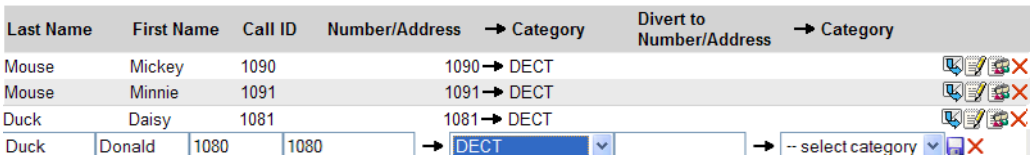
1 Click ''Users & Groups'' on the start page.

2 Select Messaging > Users in the menu on the *Configuration* page.

3 Click the ''Add'' button.

(Using the ''Advanced Add'' button gives you the possibility to create individual passwords, select user teams and create diversion rules for the user, see 4.2

Additional User Settings on page 23.).



4 Enter following settings:

Setting	Description
Last Name:	The family name
First Name:	The first (given) name
Call ID:	The Call ID can be numerical or a text string (max 50 characters). Normally the Call ID is set as the same as the handset phone number.
Number/Address:	The phone number or the personal address within selected category.
Category:	This is the messaging system to which the handset belongs (defined in the Setup Wizard). Updating or adding messaging systems is done in Messaging > Categories.
Divert to Number/Address:	The number/address to divert the message to if the Call ID is not reachable (delivery failure, absent or out of range). This is the primary destination for diverted messages. However, conditional diversions can be added after creation of the primary diversion. See 4.2.1 Advanced Diversion on page 25.
Category:	The messaging system to which the handset that shall receive the diverted messages belongs.

5 Click the ‘’ symbol to save the added user only.

Use the ‘‘Save’’ button to save all users if many users are added.

4.1.2 Add messaging users for paging

It is possible to add messaging users dedicated for paging only without consuming messaging users by mapping the users to a S900 paging category. The messaging users for paging are added in the same way as regular messaging users (see 4.1.1 Add users manually).

In this chapter will messaging users for paging furthermore be called "paging users".

In figure 8 on page 22 have two paging users been added. In the upper right corner is *plus 2 licence-free users* shown indicating that the paging users have been added without consuming any messaging users.

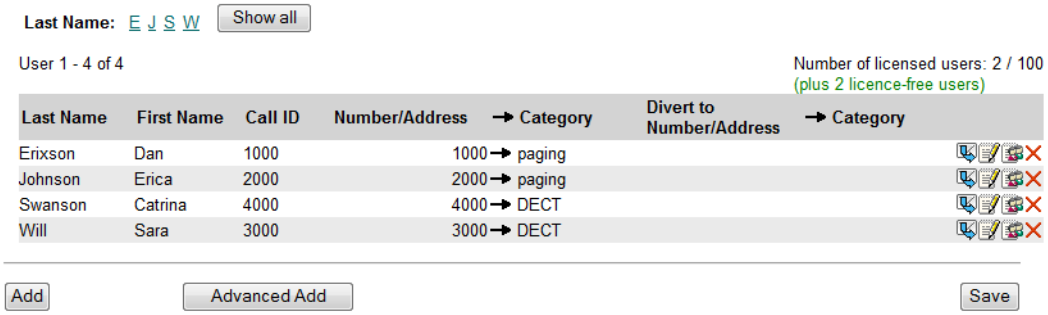


Figure 8. Paging users added without consuming regular messaging users.

When diverting a paging user to a non-paging user, the regular messaging users will be consumed. In Figure 9, a diversion for paging user 1000 has been added, where the diversion is set to a DECT user. In this case, the number of consumed messaging users increased with one and the number of licence-free users decreased with one.

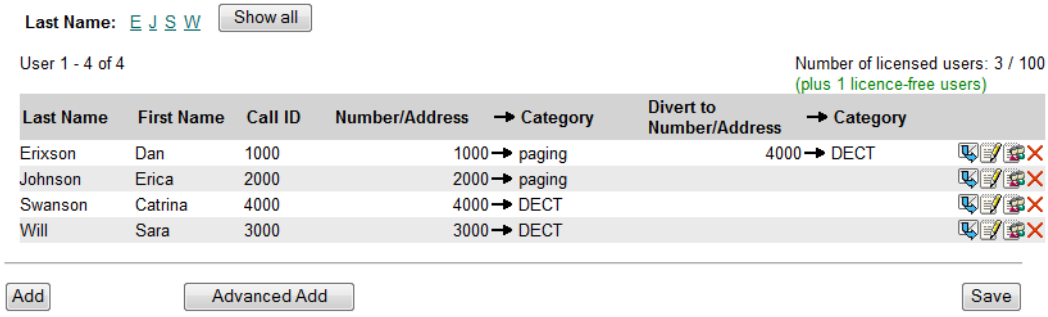


Figure 9. Diversion added for a paging user.

4.1.3 Import users from a CSV file

A CSV file template with instructions how to add user information is included in Unite CM. Obtain the template and read the instructions carefully since the user information must be added in the right order.

Obtain the CSV template

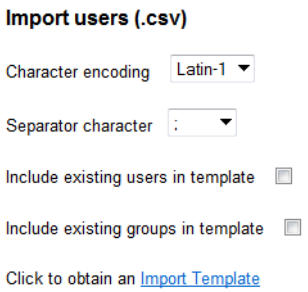
NOTE: Before obtaining the template, make sure that all needed Messaging Categories have been configured in Unite CM. The Messaging Categories will automatically be added to the template. The template only supports Latin-1 character encoding.

The template is used to easily add multiple users to the Unite CM, but the template can also be used to get an overview of the existing user information.

The existing user information included in the template cannot be edited and should be removed from the template before adding new users since existing users will not be imported. If existing user information in Unite CM needs to be edited, it must be done manually in the user interface.

1 Click ‘‘Users & Groups’’ on the start page.

2 Select Messaging > Import in the menu on the *Configuration* page



3 Select character to use as separator in the template.

4 Mark the checkbox(es) if existing Users and/or Groups is to be included in the template.

5 Click ''Import Template'' link and save the file.

6 Open the CSV file and read the instructions.

7 Add users and save the file.

Import the users

8 Click ''Browse'' to locate the CSV file.

9 Click ''Import''.

Note that user information in the CSV file only adds new users to Unite CM, it does not support editing of existing users. If user information in Unite CM needs to be edited, it must be done manually in the user interface.

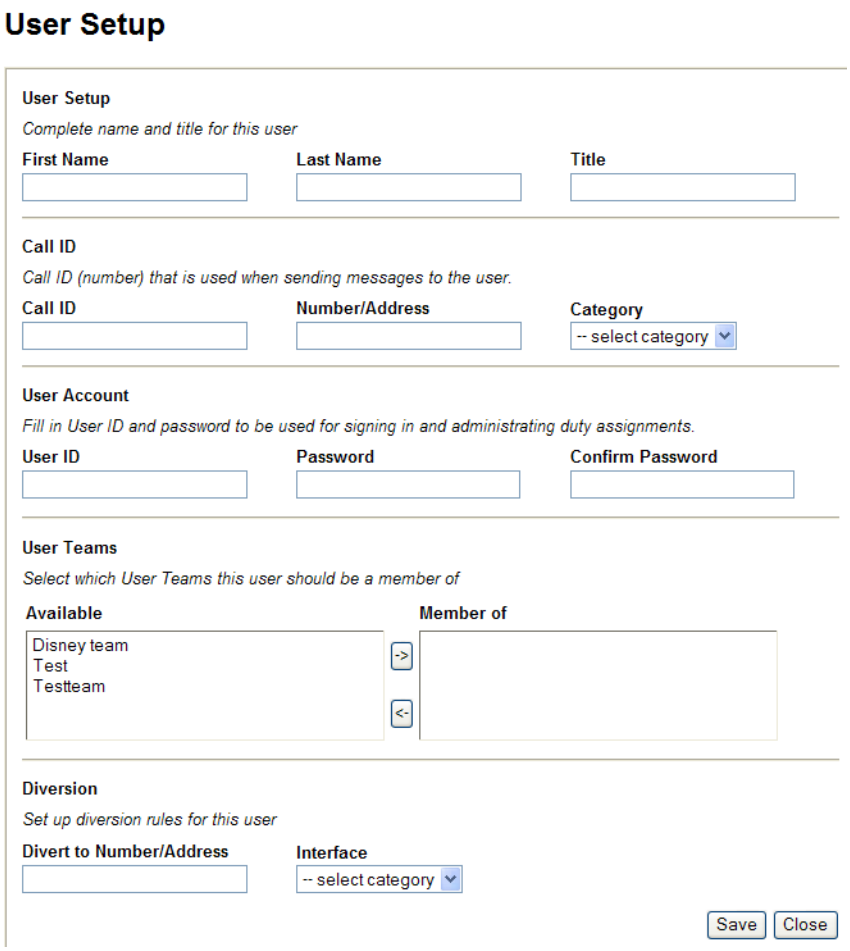
4.2 Additional User Settings

Additional user settings are set on the User Setup page. This page is reached by clicking the symbol to the right of an existing user, or by clicking the ''Advanced Add'' button for a new user.

1 Click ''Users & Groups'' on the start page.

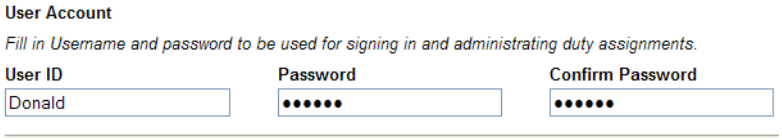
2 Select Messaging > Users in the menu on the *Configuration* page.

3 Open the *User Setup* page by clicking the symbol to the right of an existing user, or by clicking the "Advanced Add" button for a new user.



4 Enter/Edit following settings (Name, Call ID, Number/Address and Category are already set for an existing user):

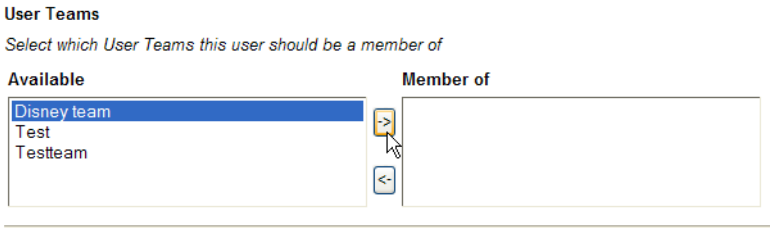
Settings	Description
First Name:	The first (given) name
Last Name:	The family name
Title:	The users title or function on the site
Call ID:	The Call ID can be numerical or a text string (max 50 characters). Normally the Call ID is set as the same as the handset phone number. This Call ID is normally used when sending message to this user from for example NetPage.
Number/Address:	The phone number or the personal address within selected category.
Category:	This is the messaging system to which the handset belongs, (defined in the Setup Wizard). Updating or adding messaging systems is done in Messaging > Categories.
User Account	
User ID: Password: Confirm Password:	A user can be given an individual User ID and password for logging in to the messaging system and for administration of duty assignments.



User Teams

Available:
Member of:

1. Mark the user team you want the user to be a member of in the Available field.
2. Click the ''->'' button to move the User Team to the Member of field.



Diversion

Diversion to other users can be set up to handle messages sent to a user that is unreachable. Messages can be diverted with direct addressing or by using the Number Plan for address look up. When direct addressing is used, the call address in the diversion condition does not have to be defined in the Number Plan. The category must however always be defined in the Number Plan.

Divert to Number/Address:

Enter a number or a personal address to divert messages to.

Interface:

The messaging system to which the handset belongs, (defined in the Setup Wizard).

5 Click ''Save''.

4.2.1 Advanced Diversion

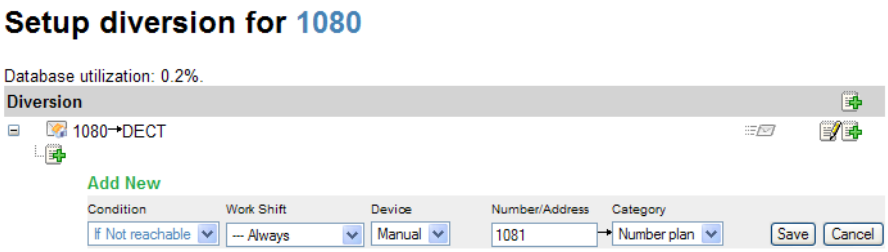
Advanced diversions can be modified to only divert messages when the handset is reported absent, out of range or not reachable, and dependent on work shift. Messages will then be sent to the specified number/address during the selected work shift only. Setting up Advanced Diversion will replace any existing simple diversion for the user. Advanced diversion can be set up for a user by clicking the symbol for the user in the Users page or by clicking the symbol and then ''Advanced diversion'' in the User Setup page.

1 Click Messaging > Users in the menu on the *Configuration* page.

2 Click the symbol to the right of the user.

3 Click the ''Advanced diversion'' button on the *User Setup* page.

4 Click the symbol to the right of the ''Edit'' symbol to add a new diversion rule.



5 The diversion is defined by a diversion condition and a destination on diversion.

Setting	Description
Condition:	Three conditions are available for diversions added below the primary diversion: - Absent, the handset is reported absent - Out of range, the handset is out of range - Not reachable, covers all message delivery failures, absent and out of range included.
Work Shift:	Messages can be diverted to different Call IDs depending on active work shift. Created work shifts will also appear in the drop-down list, but in addition two other alternatives can be selected: - Always, messages will be sent to the specified number/address regardless of active work shift. -Between shift, messages will be sent to the specified number/address to prevent messages from being undelivered if no Work Shift is active.
Device:	- Devices added for the user will be available in drop-down list. - Manual, manually enter a Call ID or number and category.
Number/ Address:	A Call ID in the number plan or a number/address
Category:	The messaging system to which the handset belongs, (defined in the Setup Wizard). Updating or adding messaging systems is done in Messaging > Categories.

NOTE: If the Number Plan is used for address look up, the category ''Number plan'' is used. If the message is diverted with direct addressing, the selected category is used.

6 Click ''Save''.

4.2.2 Create Diversion Chains

Up to 10 diversions can be added in a diversion chain. For every new diversion click the symbol after the diversion condition.

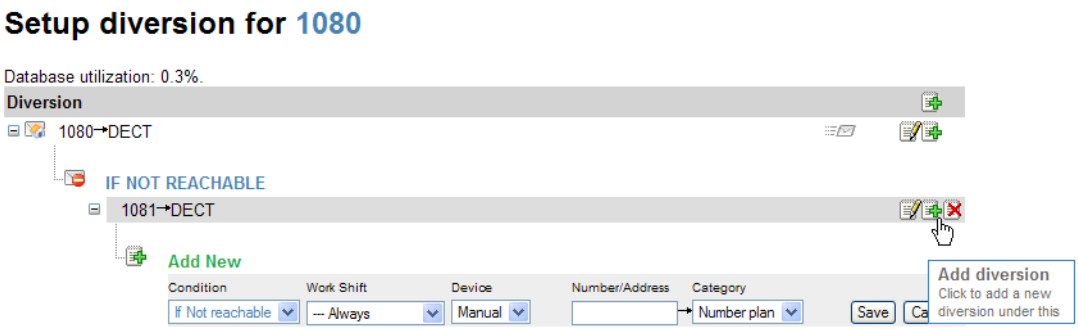
1 Click Messaging > Users in the menu on the *Configuration* page.

2 Click the symbol to the right of the user.

3 Click the ''Advanced diversion'' button on the *User Setup* page.

Add a diversion to a Not Reachable condition

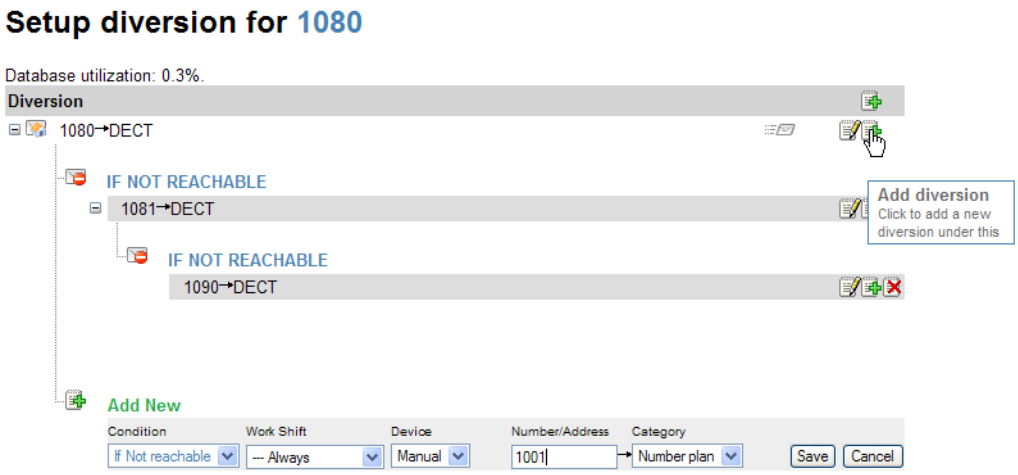
1 As shown in the figure below, click the symbol in the grey field after the destination address, in this case 1081-->DECT.



2 Enter settings and click "Save".

Add a diversion on the same level as the condition

1 Click the symbol after the primary destination, as shown in the figure below, in this case 1080-->DECT.

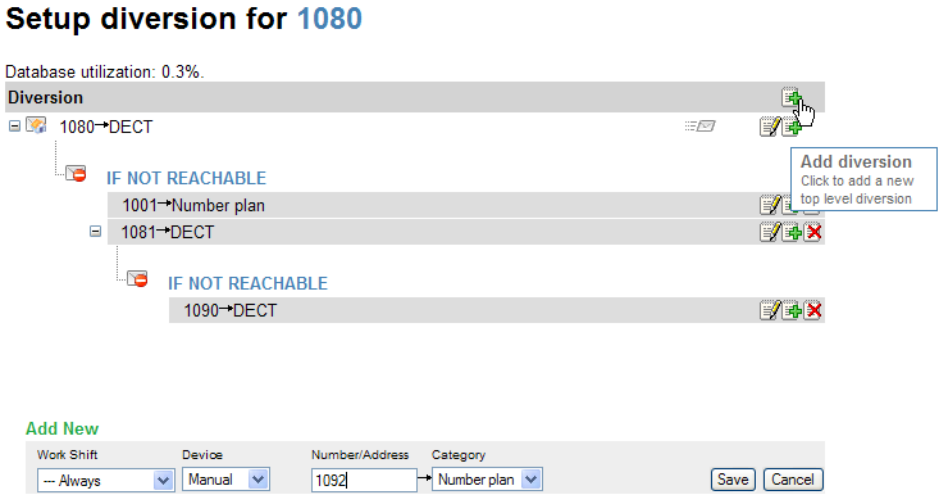


2 Enter settings and click ''Save''.

Add an unconditional diversion

1 Click the top symbol, as shown in the figure below. A secondary destination is created, meaning that all messages are directed to the primary and to the secondary destination.

The secondary destination can also have conditional diversions. It is also possible to set up diversions that depend on work shifts.



2 Enter settings and click ''Save''.

It is possible to collapse and expand the diversions by clicking the plus (+) and minus (-) symbols in the view.

Edit diversions by clicking the symbol and delete diversions by clicking the symbol.

Disable top level destination in a diversion chain

If at least one secondary destination is created, it is possible to temporarily disable the top level destination by clicking the symbol and then marking the ''Disable'' option button. At least one destination must always be enabled.

4.2.3 Additional Call IDs

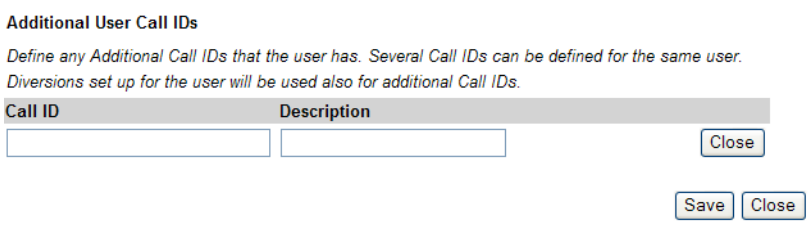
A user can have several Call IDs. An additional Call ID can be used if the users Call ID has been added as text and messages is to be sent from devices that only can handle numerical.

1 Click Messaging > Users in the menu on the *Configuration* page.

2 Click the symbol to the right of the user.

3 Click the ''Show/hide advanced settings'' button on the *User Setup* page.

4 Click ''Add new...''.


Additional User Call IDs
Define any Additional Call IDs that the user has. Several Call IDs can be defined for the same user.
Diversions set up for the user will be used also for additional Call IDs.
Call ID
Description
Close
Save
Close

5 Enter Call ID and Description in the text fields.

6 Click ''Save''.

4.2.4 Additional Devices

The user can have several devices, where the first one is the main device. Which device that should be the main one is possible to change by clicking ''Use as main''. The main device is placed first in the list.

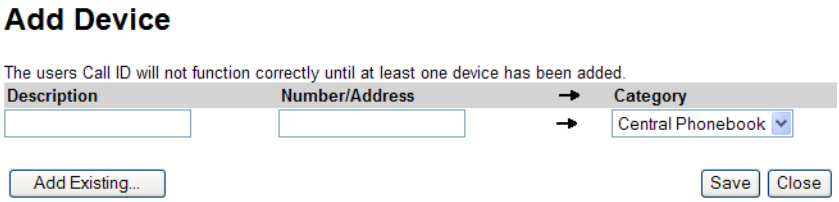
Additional devices can be used in diversion chains but it is also possible to send a message directly to an additional device by using its number/address. In that case no message is sent to the main device.

1 Click Messaging > Users in the menu on the *Configuration* page.

2 Click the symbol to the right of the user.

3 Click the ''Show/hide advanced settings'' button on the *User Setup* page.

1 Click ''Add new...''



2 Enter data in the text fields.

Setting	Description
Number/Address:	The phone number or the personal address within selected category.
Category:	The messaging system to which the handset belongs, (defined in the Setup Wizard). Updating or adding messaging systems is done in Messaging > Categories.

3 Click ''Save''.

4.3 Create Groups

Groups for the complete system are administrated in one place. The overview page gives a list of all group numbers that exist in the system. Groups make it possible to send one message to several handsets in the system.

Three different kind of group IDs can be set up:

- Group ID

  Each member in this group will receive a separate message, which means that if it is a large group it will take some time before the message has reached all members. Used for small groups (up to 10 members) and groups where delivery control is needed.
- Multicast Group ID

  In a Multicast Group one message is sent to a group number in a specified category, which means that the message is sent simultaneously to all members in the group. Used for large groups with no need of delivery control.
- Broadcast ID

  In a Broadcast Group one message is sent to a all handsets in the specified category.

  Used for sending general messages to all members.

To be able to add Broadcast and Multicast Groups there must be categories that support the corresponding function. If no such category exist, then the feature will be disabled.

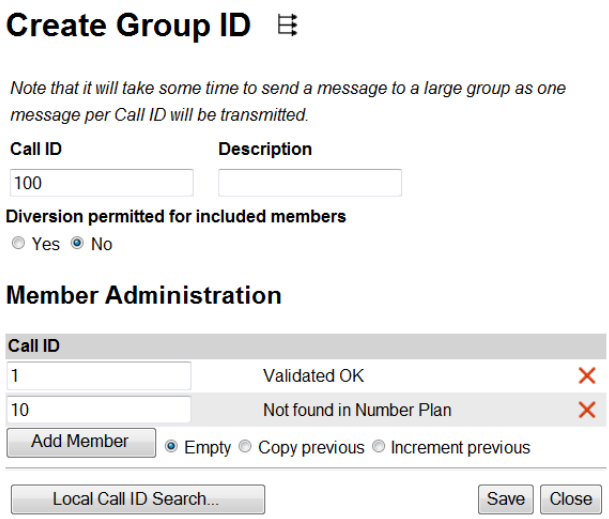
No delivery control (Multicast/Broadcast) is used since the system has no possibility to check if the message has reached all handsets.

4.3.1 Single Group

1 Click ''Users & Groups'' on the start page.

2 Select Messaging > Groups in the menu on the *Configuration* page.

3 Click ''Group ID''.



4 Enter the following settings:

Setting	Description
Call ID:	Call ID for the group
Description:	Description of the group.

Diversion permitted for included members:	Yes - Group messages will be delivered as any other messages. No - No diversion will be made for group messages

Add Members to the Group

5 Add members/handsets to the group in the Member Administration section, either by **A**) adding members one by one or **B**) search for members to add.

NOTE: The members of a Group must either have been defined as messaging user (Messaging > Users) in your Unite CM, or defined as messaging user in another Unite CM that holds the Call ID.

In the latter case, your Unite CM must be connected to the other Unite CM in order to find the corresponding Call ID when needed (that is, in a multi-site number plan solution). If the connection to the other Unite CM is lost when you adding the Call ID, an error message (with the missing Call IDs) is displayed when trying to save the group. Only save the group if you are sure that the other Unite CM will be connected later on.

A) Adding members one by one:

1 Click the ''Add Member'' button and enter the first Call ID.

When adding a Call ID, Unite CM checks if the Call ID is defined as messaging user.

2 Select if you want the next row to be ''Empty'' (default), to ''copy previous'' Call ID or ''increment previous'' Call ID by choosing an option button.

3 Click ''Add Member''.

4 Enter the next Call ID

B) Search for members to add:

1 Click the ''Call ID Search'' button.

2 Enter the first number(s) in the Call ID or Number/Address field, followed by the wildcard ''*''.
The fields can also remain empty and only category selected. Then all Call IDs in that category will be shown.

3 Click ''Search''. A list with matching Call IDs will be displayed.

4 Select users by clicking the ''Add'' button.

5 Close the UNS search list.

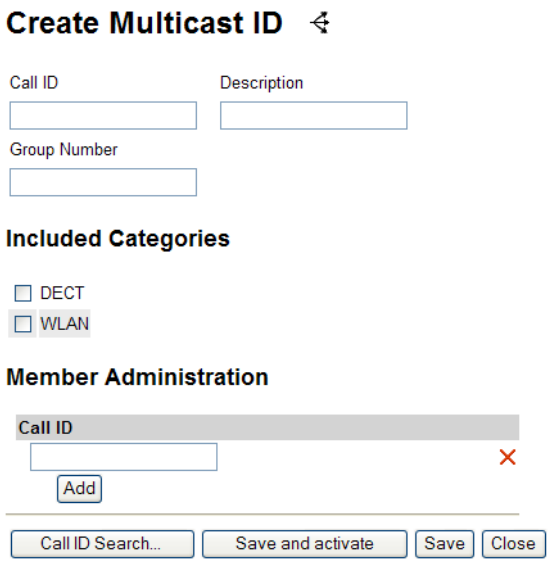
6 Click ''Save''.

4.3.2 Multicast Group

1 Click ''Users & Groups'' on the start page.

2 Select Messaging > Groups in the menu on the *Configuration* page

3 Click ''Multicast Group ID''.



4 Enter the following settings:

Setting	Description
Call ID:	Create a Multicast Group ID (numerical or a text string up to 50 characters).
Description:	Description of the multicast group.
Group Number:	The number defined in the number plan for the sub system/ radio exchange.
Included Categories:	Select category/categories. Defined in Message Routing, Category Setup.

Add Members to the Multicast Group

5 Add members/handsets to the group, in the Member Administration section, either by **A**) adding members one by one or **B**) search for members to add.

NOTE: The members (Call ID) of a Multicast group must either have been defined as messaging user (Messaging > Users) in your Unite CM, or defined as messaging user in another Unite CM that holds the Call ID.

In the latter case, your Unite CM must be connected to the other Unite CM in order to find the corresponding Call ID when needed (that is, in a multi-site number plan solution). If the connection to the other Unite CM is lost when you adding the Call ID, an error message (with the missing Call IDs) is displayed when trying to save the group. Only save the Multicast group if you are sure that the other Unite CM will be connected later on.

NOTE: A handset/Call ID can be a member in maximum eight different Multicast groups at the time.

A) Adding members one by one:

1 Click the ''Add'' button and enter the first Call ID.

2 Click the ''Add'' button again and enter the next Call ID.

3 Continue until all members are added to the group.

B) Search for members to add:

1 Click ''Call ID Search'' button.

2 Enter the first number(s) in the Call ID or Number/Address field, followed by the wildcard ''*''.
The fields can also remain empty and only category selected. Then all Call IDs in that category will be shown.

3 Click ''Search''. A list with matching Call IDs will be displayed.

4 Select users by clicking the ''Add'' button.

5 Close the UNS search list.

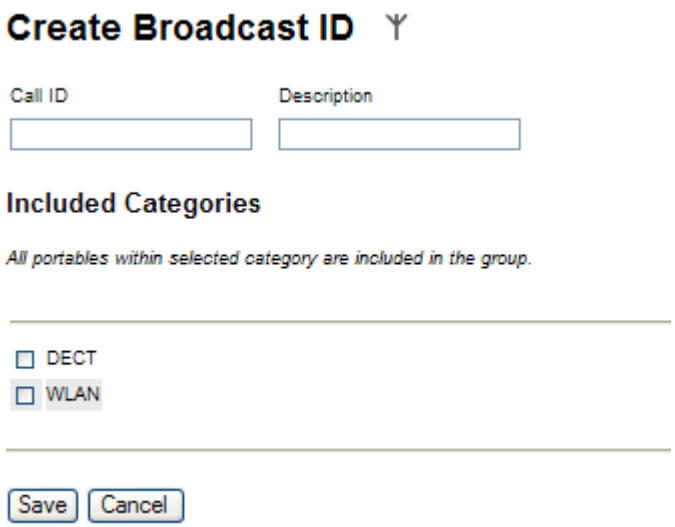
6 Click ''Save'' or, if you want to also activate the group in the carrier system, click ''Save and activate''.

4.3.3 Broadcast Group

1 Click ''Users & Groups'' on the start page.

2 Select Messaging > Groups in the menu on the *Configuration* page

3 Click ''Broadcast ID''.



4 Enter the following settings:

Call ID:	Create a Broadcast ID (numerical or a text string up to 50 characters).
Description:	Description of the Call ID (up to 100 characters)
Included categories:	Select the categories you want to include.
Category:	Defined in Message Routing, Category Setup.

5 Click ''Save''.

4.4 Create User Teams

Access rights within the system are given to User Teams. In Unite CM, messaging rights and log view rights are set up to different User Teams. One user can belong to several User Teams. To edit authorities for the User Teams, see 20.3 User Teams on page 159.

There is a default User Team that is used for logs without any connection to a user, for example a message that is sent to a handset that does not belong to any user.

1 Click Messaging > Teams in the menu on the *Configuration* page.

2 In the User Teams page, click ''Add new''.

Figure 10. Naming a new User Team.

3 Enter the name of the new User Team. The name must be unique.

4 Click ''Save''.

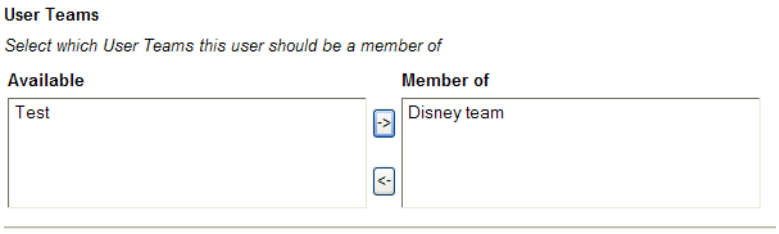
Add Members to a User Team

Users can be added to User Teams. Note that the User Team(s) must first have been created.

1 Click Messaging > Users in the menu on the *Configuration* page.

2 Click the symbol to the right of the user you want to add.

3 Select the User Team(s) you want the user to be a member of in the *Available* window and move it to the *Member of* window by clicking ''->''.



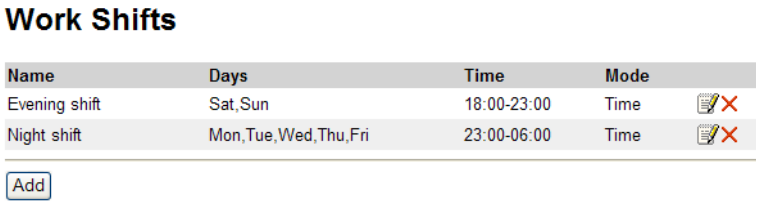
4 Click ''Save''.

4.5 Create Work Shifts

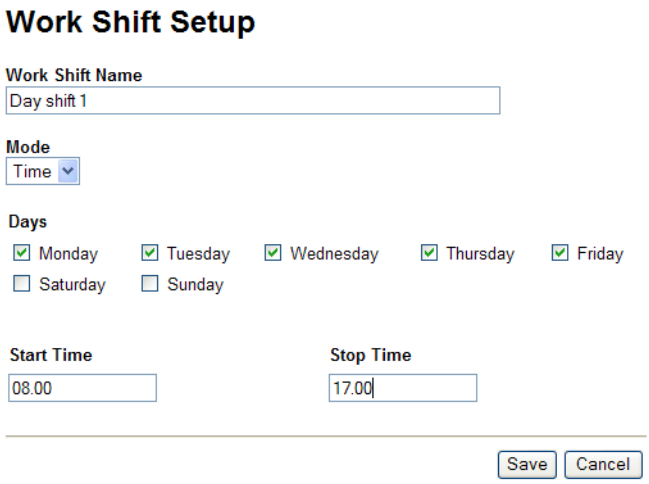
The work shifts are set up with day of week and time. The work shifts can also overlap, i.e. different work shifts can be used for different users. It is also possible to set the work shifts to be continuously On or Off, which makes it possible to test the system independent of time and day. It is also a way to solve temporary changes to shifts due to for example holidays.

1 Click Messaging > Work shifts in the menu on the *Configuration* page.

All existing work shifts will be shown in a list.



2 Click ''Add'' to set up a new work shift.



3 Enter the following settings in the text fields:

Setting	Description
Work Shift Name:	Enter the name of the work shift.
Mode:	Select shift mode; Time On – Enabled, regardless of time Off – Disabled
Days:	Which day(s) the shift shall be active.
Start Time:	When the shift shall start, for example 08.00
Stop Time:	When the shift shall stop, for example 17.00

4 Click ''Save''.

4.6 Import an ESS Backup File

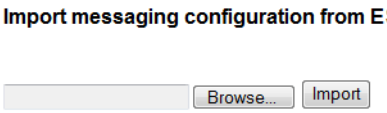
It is possible to transfer information from an ESS to a Unite CM by importing an ESS backup file. The file can include users, messaging categories, groups, devices, teams and work shifts depending on the messaging configuration of the ESS. The import of the backup file can for example be used if you want to replace the ESS with a Unite CM.

IMPORTANT: When importing the ESS backup file, the existing messaging configuration (if any) on the Unite CM will be overwritten. Diversions included in the ESS configuration will not be imported to Unite CM.

NOTE: Supported software versions of the ESS to import from is 2.30-8.3.3-A or later.

1 Select Messaging > Import in the menu on the *Configuration* page.

2 Click "Browse" and locate the ESS backup file.



3 Click "Import" to import the ESS messaging configuration.

The import of the ESS backup might take a while depending on the number of messaging users etc. to be imported.

Example:

This example describes how the information from the ESS is imported to the Unite CM.

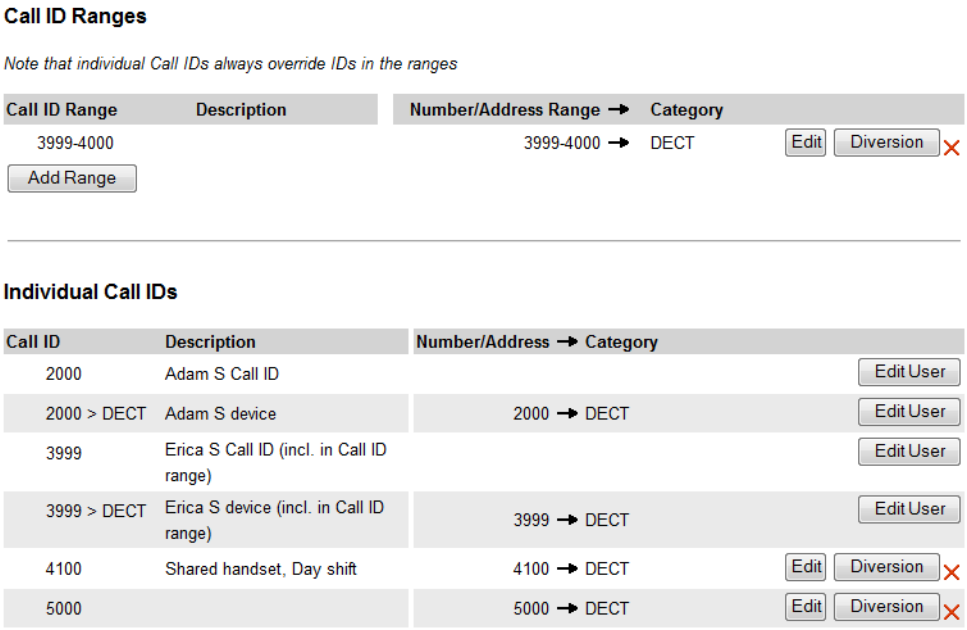


Figure 11. Example of call IDs, devices and users in ESS.

In Figure 11, the following ESS configuration is shown:

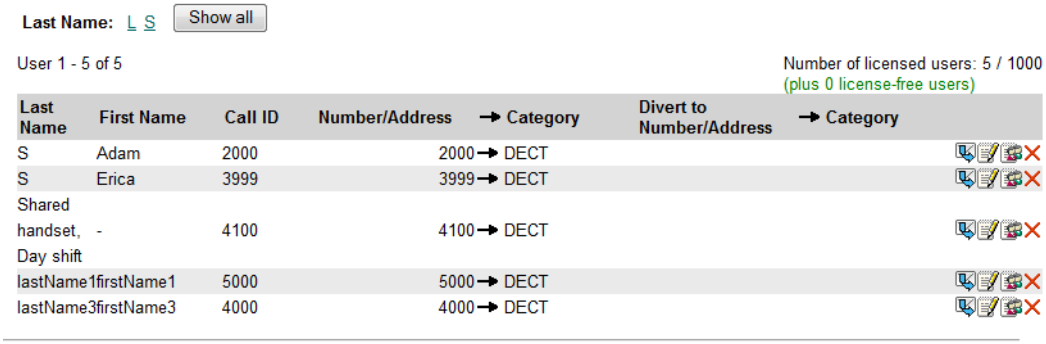
2000 Call ID and device with user associated.

3999 Call ID and device with user associated. The Call ID is also included in the Call ID range.

4000 Call ID without user associated. Only included in the Call ID range.

4100 Call ID without user associated. A description of the Call ID has been added instead.

5000 Call ID without user associated and without description.


Last Name: L S Show all

User 1 - 5 of 5

Number of licensed users: 5 / 1000
(plus 0 license-free users)

Last Name	First Name	Call ID	Number/Address	→ Category	Divert to Number/Address	→ Category
S	Adam	2000	2000	→ DECT		
S	Erica	3999	3999	→ DECT		
Shared handset, Day shift	-	4100	4100	→ DECT		
lastName1	firstName1	5000	5000	→ DECT		
lastName3	firstName3	4000	4000	→ DECT		

Figure 12. Example of imported messaging users to Unite CM.

In Unite CM, the imported ESS information appears as shown in figure 12 on page 37.

2000 Call ID, device and user imported.

3999 Call ID, device and user imported. Since the Call ID existed in the Call ID range and also as a individual Call ID, the Unite CM imported the individual Call ID only.

4000 Call ID and device imported. Since the Call ID only existed in the Call ID range, the Unite CM extracted the Call ID into an individual one.

NOTE: Extraction of Call ID ranges into individual Call IDs consumes additional messaging users in Unite CM.

In addition, since Call ID had no user associated, the Unite CM added a generic user in the format lastName<n> firstName<n>, where *n* is a number starting from 1.

4100 Call ID and device imported. Since the Call ID had no user associated but a description, the Unite CM added the description as user.

5000 Call ID and device imported. Since the Call ID had no user associated, the Unite CM added a generic user in the format lastName<n> firstName<n>, where *n* is a number starting from 1.

4.7 Manage Central Phonebook Entries

Figure 13. The Central Phonebook

The central phonebook makes it possible for users to search and find phonebook entries from a handset in the system.

NOTE: If an LDAP connection to a central phonebook is used, all settings needed is done in the Setup wizard.

If a local[1] central phonebook is used, the entries must be added, either by creating them manually, see 4.7.3 Add Entries to the Central Phonebook on page 39, or importing them from a CSV file as described below.

4.7.1 Import Entries to the Central Phonebook from a CSV File

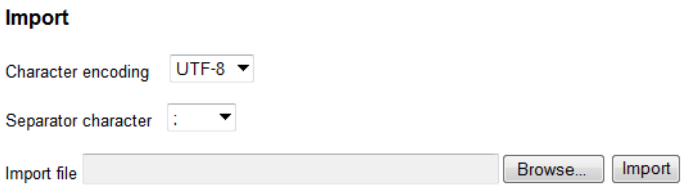
The CSV file to be imported to the phonebook should have the following format with either ";" or "," as delimiter (as in the example below) or TAB:

```
First name 1;Last name 1;Phone number 1

First name 2,Last name 2,Phone number 2
```

1 Click "Phonebook" on the start page.

2 Select Phonebook > Import/Export in the menu.



3 Select the character encoding of the file in the *Character encoding* drop-down list.
NOTE: It is important that you select the same character encoding that the file is saved as. If not, the entries will be corrupted after the file has been imported.

4 Select the separator for the file in the *Separator character* drop-down list.

5 Click "Browse" to locate the CSV file in the system.

NOTE: The existing entries (if any) will be overwritten when importing the CSV-file.

6 Click "Import".

4.7.2 Export the Central Phonebook to a CSV File

The complete central phonebook can be exported to a CSV file for example for editing or backup reasons. The exported file will be saved with the character encoding UTF-8.

1."Local" means that the entries are stored in Unite CM, instead of storing the entries on an LDAP or CMG database.

1 Click ‘‘Phonebook’’ on the start page.

2 Select Phonebook > Import/Export in the menu.

3 Click ‘‘Export’’.

4 Click ‘‘Save’’ in the dialog window that appears.

5 Enter a name of the file and select in which folder the file should be saved and click ‘‘Save’’.

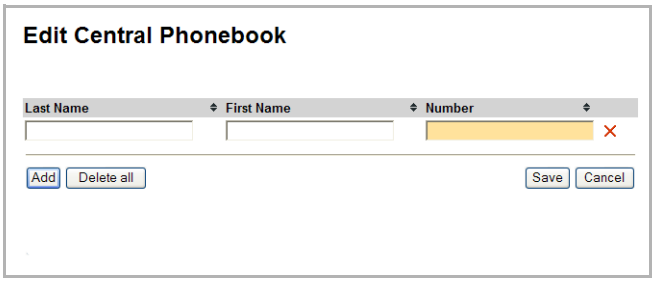
4.7.3 Add Entries to the Central Phonebook

The entries in the central phonebook can be filled in manually. The central phonebook supports entries with character encoding UTF-8 (for example Russian characters and Swedish characters).

1 Click ‘‘Phonebook’’ on the start page.

2 Select Phonebook > Edit in the menu.

3 Click ‘‘Add’’.



4 Enter the following settings in the text fields:

Setting	Description
Last Name:	The family name
First Name:	The first (given) name
Number:	The phone number

5 To add several rows click ‘‘Add’’ again.

6 Click ‘‘Save’’.

4.8 Input/Output Setup

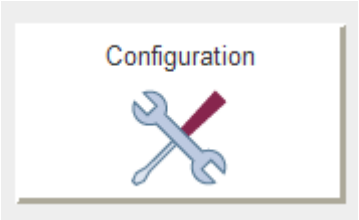


Figure 14. Configuration

Inputs and outputs are defined in the I/O Setup page found in the left menu under ''Other''. The activation of an input can be set to ''on opening'' or ''on closing'', and the initial state for the output can be set to ''Low'' or ''High''.

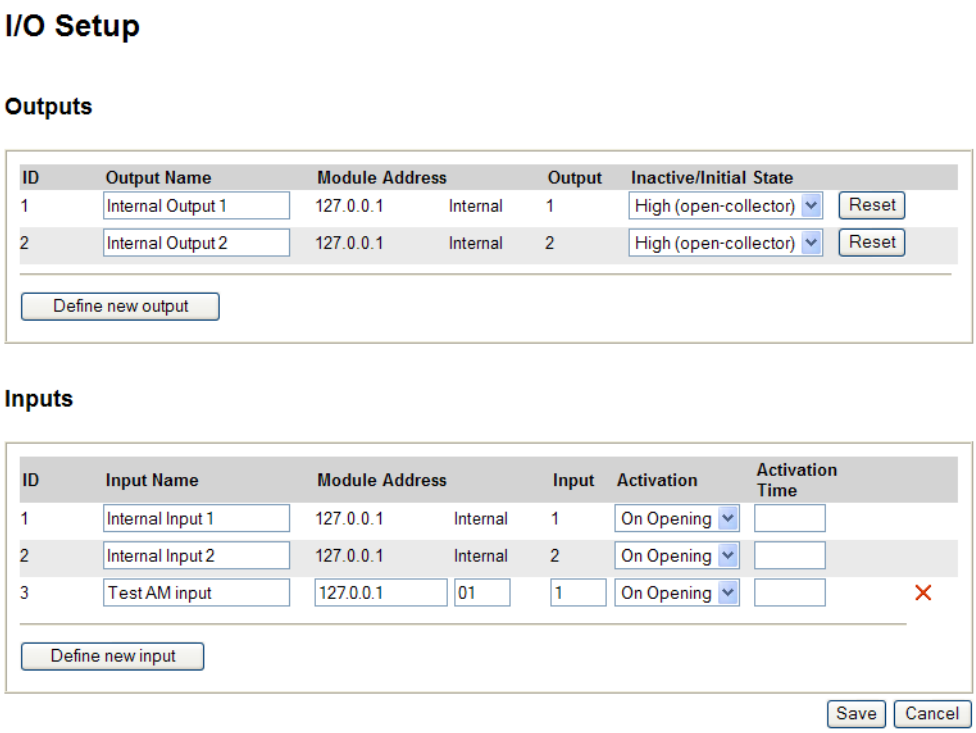


Figure 15. I/O Setup page

For the outputs, the state is set to the opposite of the initial state when activated. For example; if Output 2 is set to "Low" in initial state, the output will automatically be set to "High" when activated.

Every time a new output or input is defined, an automatic ID is created. The ID is a running number which can manually be changed into another number or a text if wanted. When an output or input has been deleted, Unite CM will not remember that the previous ID number is free to be used again. The numbering will just continue on the number after the last created one.

4.8.1 Defining Inputs and Outputs

Before an input or output can be used in the configuration, it has to be defined with a name and Module Address. The module address consists of IP address, and if Alarm Module and/or Output Module are used, the module address on the A-bus.

Unite CM inputs

Unite CM hardware has two inputs that can be used. These inputs are predefined at delivery. The states that can be detected are open and close.

Unite CM outputs

Unite CM hardware has two outputs of open-collector type that can be used in the Alarm Handling and Fault Handling. These outputs are predefined at delivery. The initial state can be set to high or low.

Alarm Module inputs

The number of inputs that can be used can be extended by using an Alarm Module (AM) connected to the A-bus. The input on the AM is defined by a name, the IP address of the Unite module connected to the A-bus, the AM's module address[1] on the A-bus, and the input number. The states that can be detected are open and close.

Output Module outputs

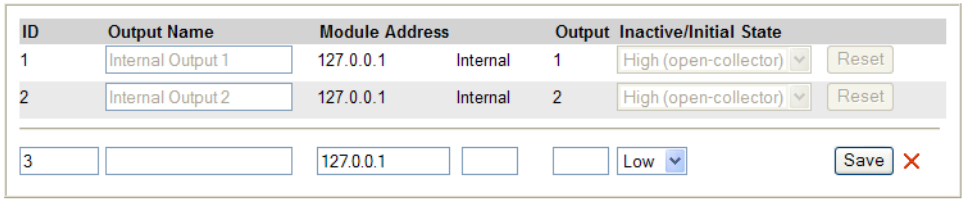
The number of outputs that can be used in Unite CM can be extended by using an Output Module (OM) connected to the A-bus. The output on the OM is defined by a name, the IP address of the Unite module connected to the A-bus, the OM's module address[1] on the A-bus and the output number. The initial state can be set to high or low.

For more information refer to the hardware Installation Guide, Elise3, TD 92679GB.

4.8.2 Define Output

1 Click Other > Input/Output

Outputs



2 Click "Define new output".

3 Enter a unique Output Name.

4 Enter IP address of the module connected to the A-bus.

Normally loopback to localhost (that is, the IP-address is set to 127.0.0.1), but if the A-bus is connected to another Unite module its IP address is set here.

5 Enter the Output Module's (whose output should be activated) "module address" on the A-bus

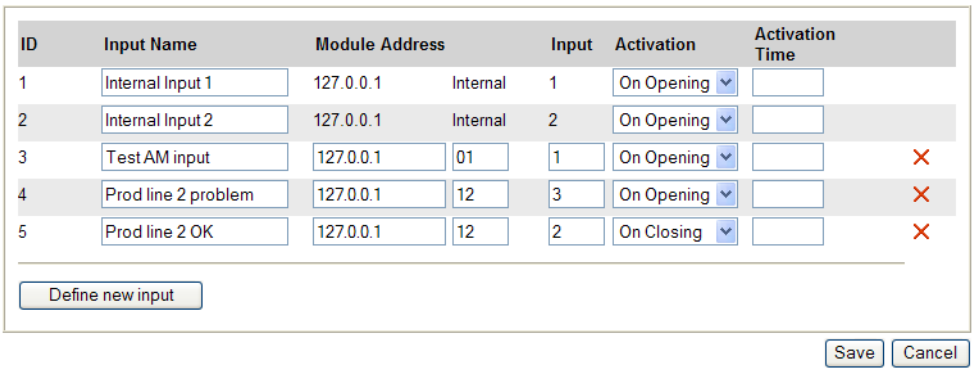
6 Enter Output number.

7 Select Initial State and click "Save".

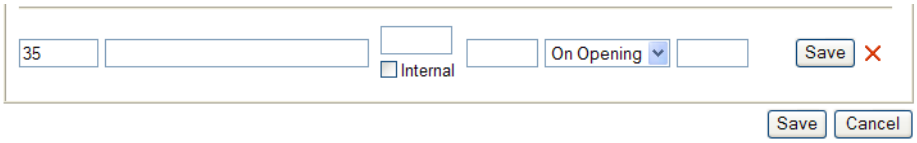
1.Every module that is connected to the A-bus has a two digit hexadecimal address that is set with a DIP switch.

4.8.3 Define Inputs

Inputs


ID
Input Name
Module Address
Input
Activation
Activation Time
1 Internal Input 1 127.0.0.1 Internal 1 On Opening
2 Internal Input 2 127.0.0.1 Internal 2 On Opening
3 Test AM input 127.0.0.1 01 1 On Opening
4 Prod line 2 problem 127.0.0.1 12 3 On Opening
5 Prod line 2 OK 127.0.0.1 12 2 On Closing
Define new input
Save
Cancel

1 Click ''Define new input''.



2 Enter a unique Input Name.

3 Enter IP address of the module connected to the A-bus.

Normally localhost (that is, the IP address is set to 127.0.0.1), but if the A-bus is connected to another Unite module its IP address is set here.

4 Enter the Alarm Module's ''module address'' on the A-bus or select ''Internal'' depending on if the input is connected via A-bus module or directly to Unite CM hardware.

If you want to trigger on both opening and closing or using different ''Activation time'', you can define multiple inputs for the same physical input. This can for example be used if you at a door (by using a microswitch) want an activation on both opening and closing the door. Refer to Appendix F for other examples.

5 Enter Input number.

Note: If you have selected the internal check box in the previous step, enter the number of the internal input (1 or 2).

6 Select Activation condition.

7 Enter Activation Time. By default, a notification will be sent immediately. If you enter activation time, the input has to be active for the set time before a notification is sent.

8 Click ''Save''.

4.8.4 Input Activity Distribution

If the Unite CM's input port(s) is activated, the Unite CM can trigger other services by distributing the input activity to the services. The services in turn can then determine which action to be performed depending on their settings.

The default services are SystemSurvey, EventHandler, OAJ, and BasicAlarmHandler. Note that the default services might be license dependent. If your Unite CM does not have license(s) for the service(s), remove the service(s) from the list to avoid fault messages in the Unite CM's fault log.

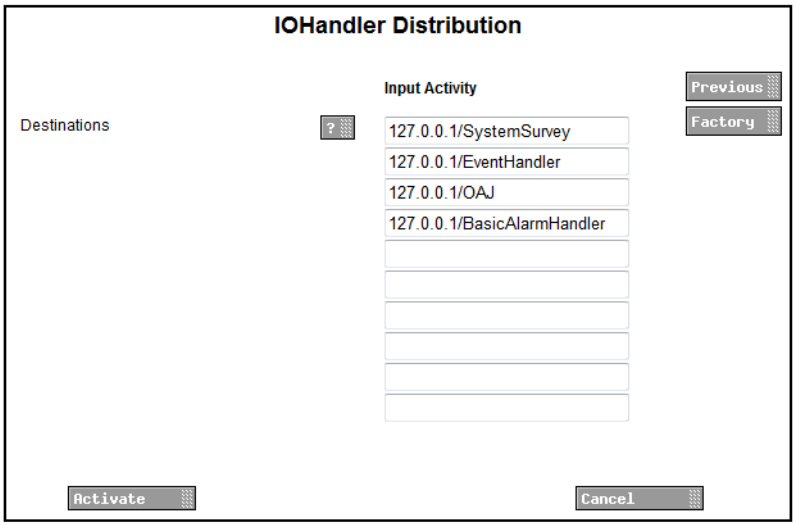


Figure 16. Default Input Activity Distribution List

1 Make sure that inputs have been defined according to 4.8.3 Define Inputs on page 42.

2 Click "Configuration" on the start page.

3 Select Other > Advanced Configuration. The *Advanced Configuration* page opens.

4 Click "Input Activity Distribution" under Other.

5 Enter the destination address(es) to the service(s) to be used. The address format is IP address/service.

4.9 Alarm Handling

The alarm handling included in Unite CM makes it possible to trigger on alarms and data from handsets. Activated inputs on Unite CM, or a module connected to the A-bus, can also be used as a trigger. As an action to the incoming information, messages can be sent to handsets. Messages with character encoding UTF-8 (for example Russian characters and Swedish characters) are supported.

Besides messages, it is also possible to activate outputs on Unite CM or modules connected to the A-bus.

There are two ways of configure triggers and actions. The Basic Alarm Manager (BAM) can be used for the most common triggers/actions (see 4.10 Basic Alarm Manager on page 45). If you want to configure other triggers/actions that are not included in the BAM, you can program own triggers/actions by using the Event Handler (see 4.11 Advanced Event Handling on page 51).

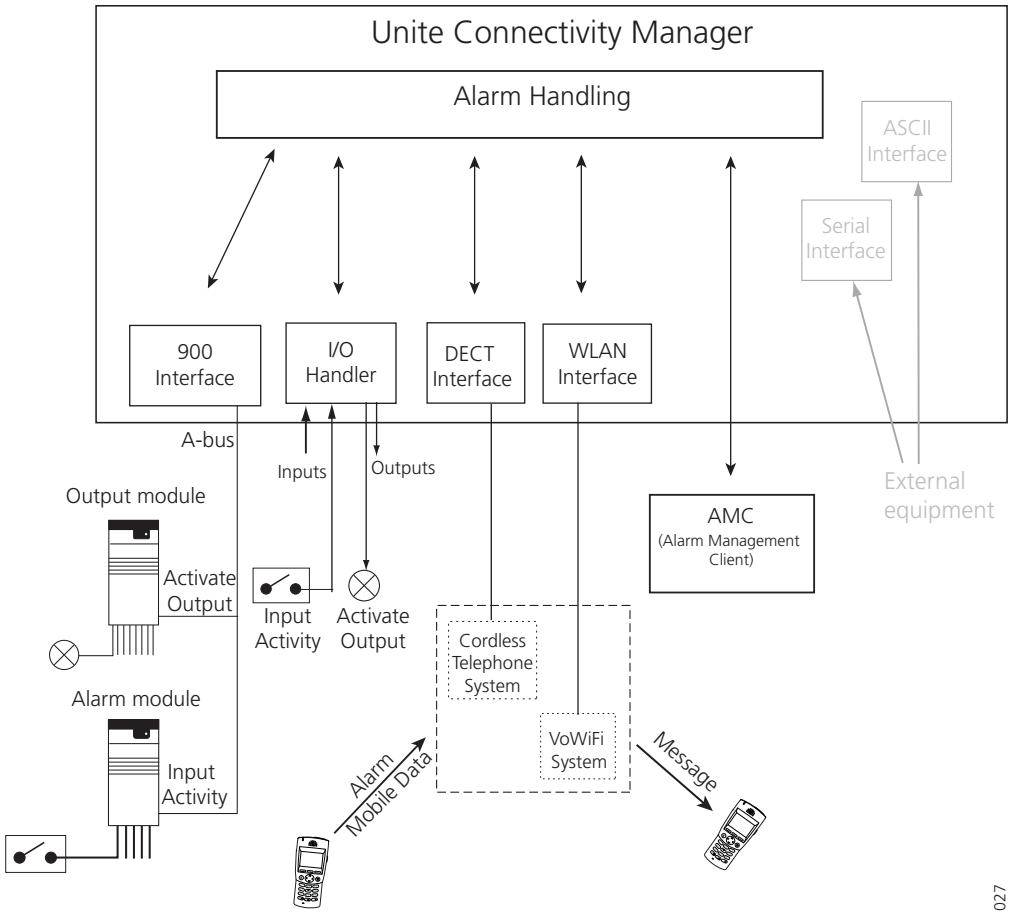


Figure 17. Communication flow for the Alarm Handling and external systems.

4.9.1 Nomenclature

Alarm action: An alarm action consists of trigger conditions that leads to an action. For example, sending a message to a handset in the system and/or activating an output. One alarm action can consist of several triggers and lead to several actions. The actions can be repeated at a regular time interval as long as an input is active.

Input: An input on Unite CM or an input on an Alarm Module, connected to the A-bus.

Output: An output on Unite CM or an output on an Output Module, connected to the A-bus.

Trigger: A trigger is a set of conditions that have to be fulfilled, for example that an input has to be open for a certain time period or that an alarm has been sent from a handset.
Several triggers of the same type can be defined for each alarm action. The actions will be carried out when any of the triggers is fulfilled.

Action: Sending a message to a handset, activating an output or initiating a push-to-talk (PTT) conference call.

Escalation: If a message with confirmation request has not been accepted within the set number of seconds, an escalation action can be started. If several messages were sent, the escalation will be cancelled as soon as one of them is accepted.
If, on the other hand, the message is rejected by all recipients, the escalation will start immediately. Up to three escalation levels are possible.

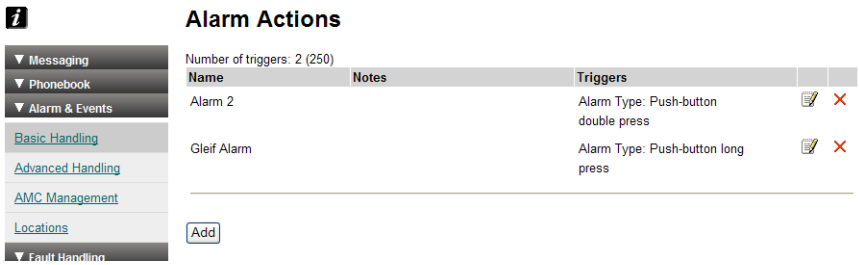
4.10 Basic Alarm Manager

The Basic Alarm Manager (BAM) is a basic tool that allows the user to simply determine what should trigger an alarm and which action to be done after the alarm.

TIP: If you want to configure trigger/action that is not included in the BAM, use the Event Handler instead. See 4.11 Advanced Event Handling on page 51.

4.10.1 Add Alarm Actions

1 Select Alarm & Events > Basic Handling.



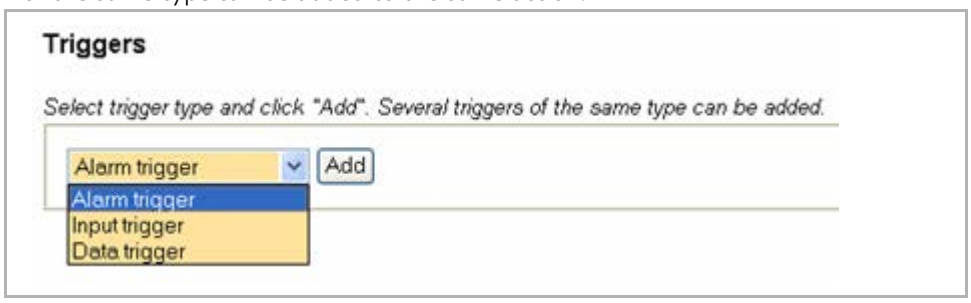
2 Click "Add".

3 Enter a descriptive name for the alarm action in the *Name* text field.

4 Enter a short description/useful information in the *Notes* text field.

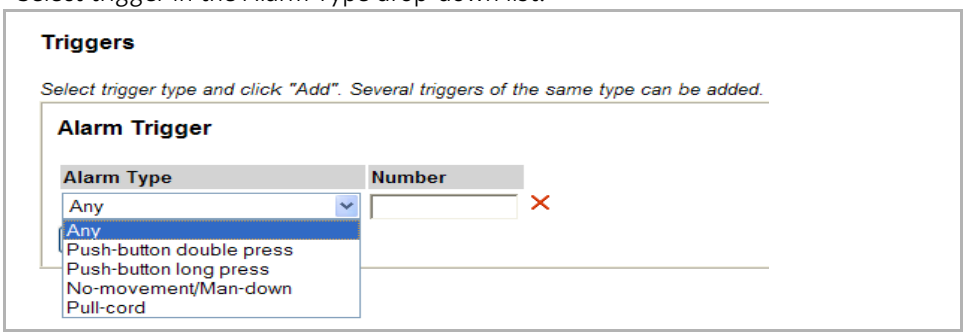
Define Trigger

1 Select type of trigger in the Triggers drop-down list and click ''Add''. Several triggers of the same type can be added to the same action.



- Alarm Trigger

1 Select trigger in the Alarm Type drop-down list.

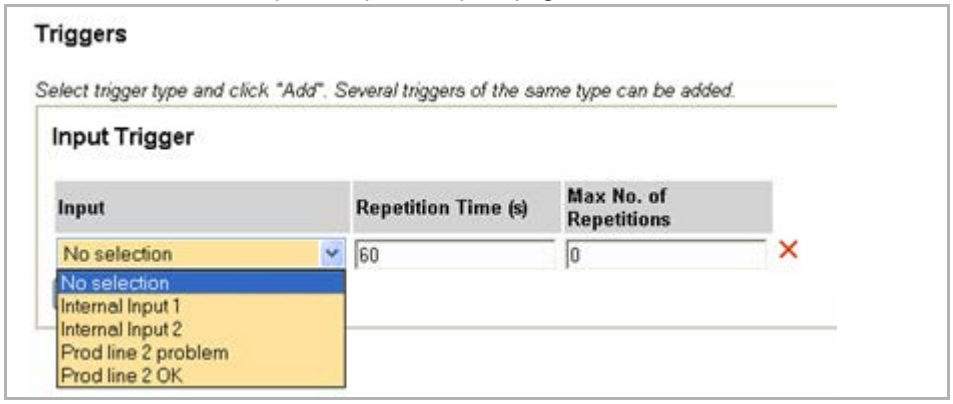


2 If the alarm is to be sent from a specific handset, enter handset no. in the Number text field. Leave empty if any handset shall be able to trigger the alarm. Note that the handset must be defined in Messaging Users.

3 Click ''Add''.

- Input Trigger

1 Select input in the Input drop-down list. Only inputs defined in the I/O Setup are available. Refer to 4.8 Input/Output Setup on page 39.



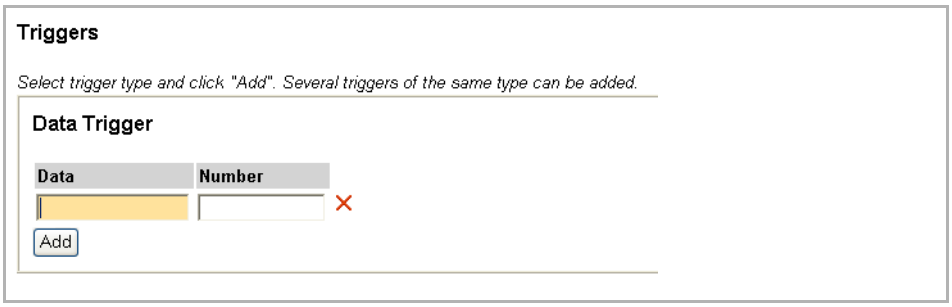
2 Enter (in seconds) the interval between repetitions in the Repetition Time text field. Note that this field must be set to min. 10 seconds even if no repetitions shall be made.

3 Enter how many times the action shall be repeated in the Max. No. of Repetitions text field. For no repetitions, enter ''0''.

4 Click ''Add''.

- Data Trigger

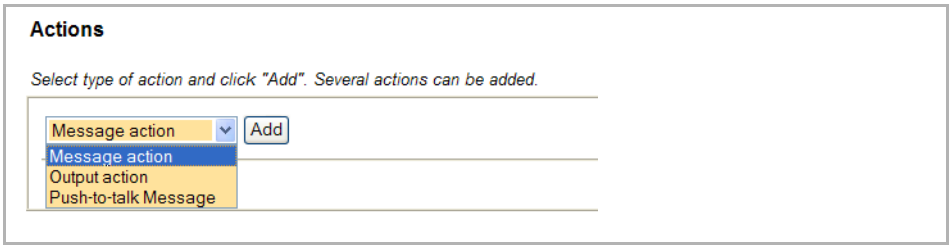
1 Enter data in the *Data* text field.



2 If the data is to be sent from a specific handset, enter handset No. in the Number text field. Leave empty if any handset shall be able to send the data. Note that the handset must be defined in Messaging Users.

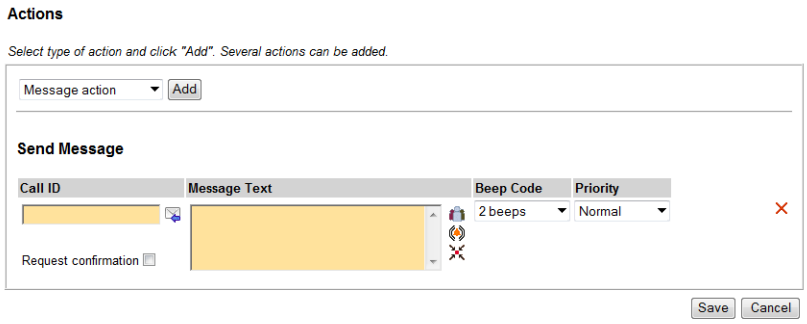
Select Type of Action

1 Select type of action in the Actions drop-down list and click ''Add''. Several actions can be added.



- Message Action

NOTE: The Call ID must be defined as a messaging user in a Unite CM connected to your system. For example, if several Unite CMs are connected, the "local" Unite CM does not need to have the Call ID in its number plan. In this case, the local Unite CM must be connected to another Unite CM that holds the Call ID.



1 Do one of the following:

- In the *Call ID* text field, enter the Call ID that should receive the message.
- Click the symbol, to the right of the *Call ID* text field, if the message is to be sent as a reply to the sender of the alarm or data.

2 Enter the message text in the *Message Text* field. By clicking the symbols to the right of the text field, you can add valuable information to the message, such as Call ID of the sender, type of alarm and the location.

If an input is activated the description of the input can be added.

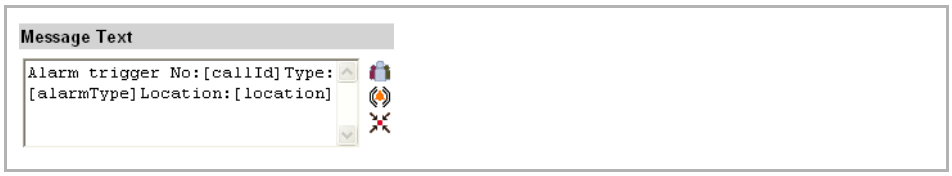


Figure 18. Available information for the alarm trigger

Figure 19. Available information for the input trigger

Figure 20. Available information for the data trigger

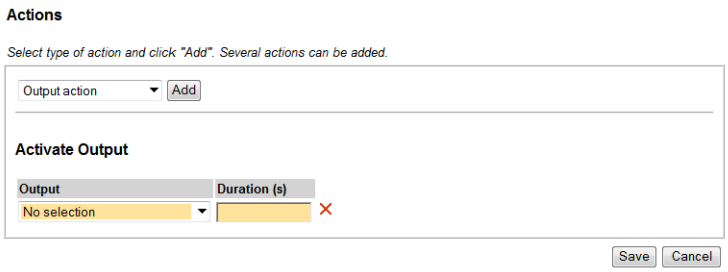
3 Select number of beeps in the *Beep Code* drop-down list.

4 Select message priority in the *Priority* drop-down list.

5 Select the Request confirmation check box if it shall be possible for the user to accept or reject the message. If no response is received an escalation action can take place, refer to Select Escalation Action on page 50.

- Output Action

1 Select which output to activate in the Output drop-down list. Only outputs defined in the I/O Setup are available. Refer to 4.8 Input/Output Setup on page 39.

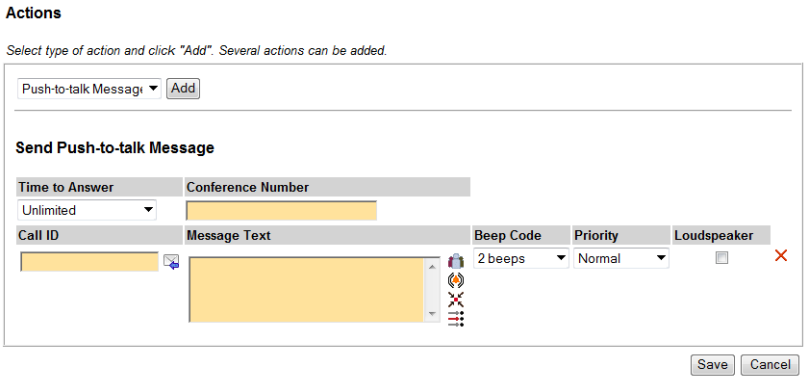


2 Enter (in seconds) for how long the output shall be activated in the Duration text field.

- Push to talk (PTT) Message

A PTT message makes it possible to set up a conference call. When a PTT message is manually accepted by the user, the handset connects to the conference number and the handsets involved in the conference are connected.

1 Select the time (in minutes) the receiving handset shall have the possibility to join the conference, in the *Time to Answer* drop-down list.



2 Enter the number to the conference group in the *Conference Number* text field.

3 Do one of the following:

- Enter the Call IDs that shall receive the Push-to-talk message in the *Call ID* text field. Each Call ID shall be separated with a comma.
- Click the symbol, to the right of the *Call ID* text field, if the message is to be sent as a reply to the sender of the alarm or data.

NOTE: The Call ID must be defined as a messaging user in your Unite CM. If a multi-site number plan is used, the Unite CM that holds the Call ID must have the messaging user defined instead.

4 Enter the message text in the *Message Text* field. By clicking the symbols to the right of the text field you can add valuable information to the message, such as Call ID of the sender, type of alarm and the location.

If an input is activated the description of the input can be added.

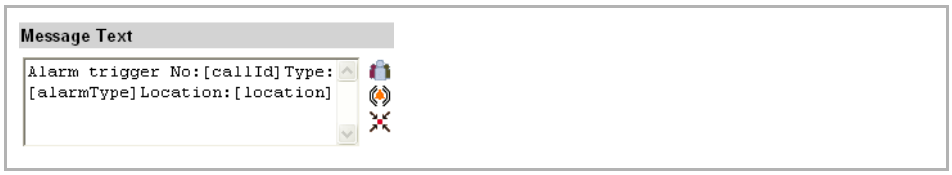


Figure 21. Available information for the alarm trigger

Figure 22. Available information for the input trigger

Figure 23. Available information for the data trigger

5 Select number of beeps in the *Beep Code* drop-down list.

6 Select message priority in the *Priority* drop-down list.

7 If the loudspeaker mode on the handset shall be activated when a user has accepted the PTT message, tick the *Loudspeaker* check box.

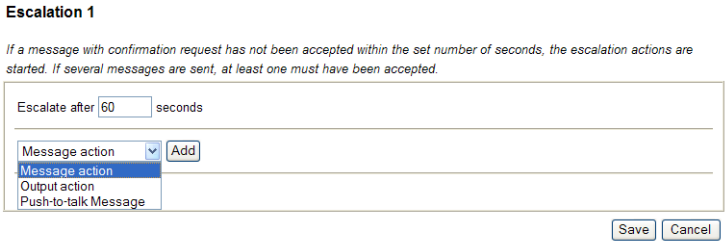
8 Click Save

Select Escalation Action

If the Request confirmation check box is checked and the message has not been confirmed within the specified time, it can be escalated to another action which in turn can be escalated. Up to three escalations are possible for each triggered alarm action.

Note: If the input trigger is repeated make sure the Repetition Time, refer to • Input Trigger on page 46, is longer than the complete escalation chain. This is advised to avoid confusing the users with several simultaneous escalation chains for the same trigger.

1 Enter (in seconds) for how long Unite CM shall wait before escalation.


Escalation 1
If a message with confirmation request has not been accepted within the set number of seconds, the escalation actions are started. If several messages are sent, at least one must have been accepted.
Escalate after 60 seconds
Message action
Add
Message action
Output action
Push-to-talk Message
Save
Cancel

2 Select action to take in the Escalation drop-down list and click ''Add''.

- For Message action refer to • Message Action on page 47.
- For Output action refer to • Output Action on page 48.
- For Push-to-talk Message refer to • Push to talk (PTT) Message on page 49.

3 Click ''Save''.

4.10.2 Add Locations

IMPORTANT: Do not mix the two location types DECT location and Base Station location in one system.
When the Alarm Handling on Unite CM triggers on ''Alarm trigger'' the included location in a text message action can be faulty because DECT location is prioritized higher then Base Station location. That is if a handset has received a DECT location in one area and the user sends an alarm from another area with only Base Station locations, the location that will be included in the message text is the DECT location that could be very old and no longer valid.

1 Select Alarm Handling > Locations and click ''Add''.

2 Enter the code for the location in the Code text field.

Tip: To get the code for the location: 1) select alarm trigger, 2) create a message action, 3) click ''Reply to sender'' icon to send the message to the sender of the alarm, 4) insert [location] in the message text, 5) trigger an alarm. You will receive the code in the display.

3 Enter a short description of the location in the Description text field. Click ''Save''. When setting up the alarm action this description can be included in the message text.

4.11 Advanced Event Handling

Unite CM includes an Event Handler which makes it possible to set up actions on incoming events such as mobile data, alarm, activation of an input, etc.

Different actions depending on the incoming event, can then be performed by Event Handler. Actions can be both internal, that is, start other Actions after a delay; and external, that is, send a message, start a siren, or to present information about the alarm in an Alarm Management Client (AMC).

4.11.1 Planning

Before implementation of actions and events, it is necessary to plan and identify actions and events etc. that is going to be set up in the GUI. If Duty Assignment is going to be used you also have to consider about user teams, location layout, and access rights.

For best result, follow the step-by-step guide:

1 Identify external Events that shall result in an action.

2 Which actions are needed for the Event.

3 Which information are needed in the actions.

4 Define escalation chain, and success/failure conditions.

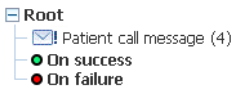


Figure 24. Example of an escalation chain with success/failure conditions

5 If Duty Assignment is going to be used, create location layout and related information.

6 Define required conversion tables.

7 If Duty Assignment is going to be used, Users and User Teams have to be defined and Access Rights for the User Teams.

When this is done the administration of the User Interface can be started. See User Manual, Action Assignment in Unite Connectivity Manager, TD 92842EN on how to configure and administrate.

4.11.2 Action Handler

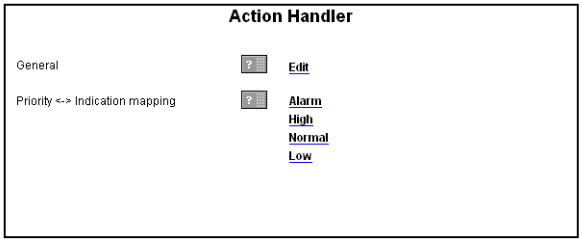
If more than one Unite CM is used it must be defined which module that shall handle event assignments. Message indications can be modified dependent on the priority of the message.

Different priority levels can be given different beep signals and be mapped to different colors as an additional indication to the recipient of the message. The priority color will be shown in the receiving device which can be a handset or the *View* application in *Ascom Unite Messaging Suite for Healthcare*.

1 Click ''Configuration'' on the start page.

2 Select Other > Advanced Configuration in the left menu in the *Configuration* page.

3 Click ''Action Handler'' in the menu on the *Advanced Configuration* page.



General parameters

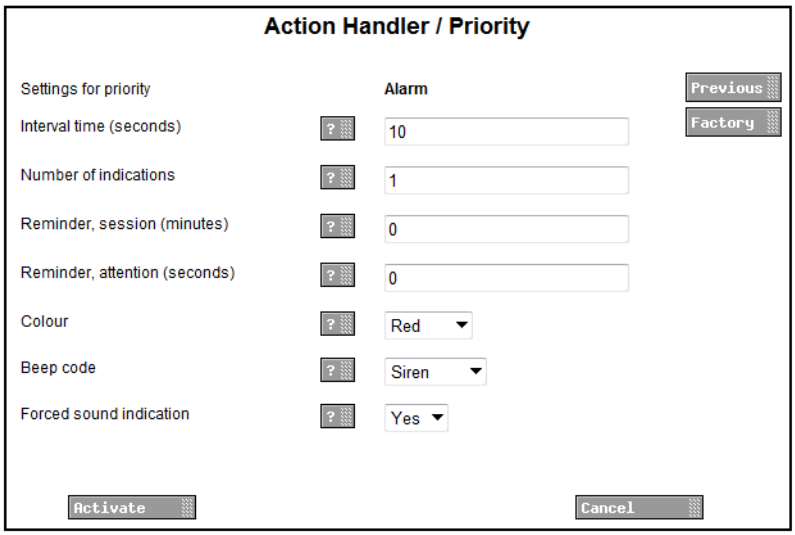
4 Click ''Edit''.

5 Following general parameters can be set:

Settings	Description
Assignment Handler IP address:	Enter the IP address of the Action Handler that shall handle event assignments.
Identity:	A unique name for the Action Handler should be entered when more than one Unite CM is used.
Individual group number response:	Set to ''Yes'' if an action sent to an address, that is diverted to two or more members, shall wait for responses from all members before deciding the action to be a failure.
Report status:	Set to ''Yes'' if status for all actions sent from the Action Handler shall be reported back to the Event Handler.

6 Click ''Activate''.

Priority <-> Indication mapping



1 For each priority (Alarm, High, Normal and Low) the following parameters can be set:

Settings	Description
Interval time (seconds):	Determines the time to be elapsed between each repetition of the indication.
Number of indications:	How many times the indication shall be repeated
Reminder, session (minutes):	Determines the time to be elapsed between each indication before a reminder of the indication is sent to the device. The reminder will only work if the message has not been deleted in the device.
Reminder, attention:	Time between indications before message is selected
Colour:	Determines which color coding messages with this priority shall have.
Beep code:	Determines which default beep code messages with this priority shall have. The setting might be overridden in the individual messages, defined in Action Configuration.
Forced sound indication:	Determines if sound indication for messages with this priority level (High, Normal, and Low) always shall breakthrough in a device, even though the device is set to silent. NOTE: Use this parameter with care. It is strongly recommended to only enable this parameter for messages that really have to breakthrough in a silenced device. Messages with alarm priority level will always breakthrough in a silenced device regardless of this setting.

2 Click ''Activate''.

4.11.3 Event Handler

The Event Handler makes it possible to set up actions on incoming events. An event can be mobile data, an alarm, activation of an input, etc. The Event Handler will then perform different actions depending on the incoming event. Actions can be both internal, that is,

start other Actions after a delay, and external, i.e. send a message, start a siren, or present information about the alarm in the Alarm Management Client (AMC).

In the Event Handler there are four different links, where events and triggers are set up for Event Elements, an overview of the programming, to view Event Handler logs, and where to administrate the data bases of the Event Handler.

More information about the configuration of the Event Handler is found in the document, Programming Guide, Event Handler, TD 92329GB.

1 Click ''Configuration'' on the start page.

2 Select Alarm & Events > Advanced Handling in the menu on the *Configuration* page.

Figure 25. Links to the Event Handler

Programming Overview

The Overview shows an overview of the Event Handler programming, which can be a help during programming.

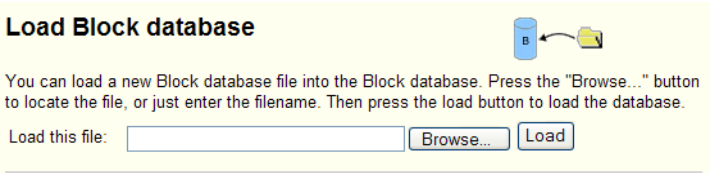
View Logs

All changes in the configuration of the Event Handler are written to the log. It is also possible to write information to the log, for example when a trigger is activated. For more information about the log file and its content, see the chapter Event Log File in the Programming Guide, Event Handler, TD 92329GB.

Administration

The database administration is used to synchronize the Event Elements that have been created in the Event Assignment User Interface.

1 Click Administration, and go to Load Block database, located at the bottom of the page.


Load Block database
You can load a new Block database file into the Block database. Press the "Browse..." button to locate the file, or just enter the filename. Then press the load button to load the database.
Load this file:
Browse...
Load

2 Locate the database file and click ''Load'', a dialogue window opens.

3 Click ''Yes'' to synchronize.

4 Go back to the Advanced Handling and Event Handler, see 5.13.4 Configuration of Events.

4.11.4 Configuration of Events

This is used to make assignment of Event Elements.

1 Click Configuration.

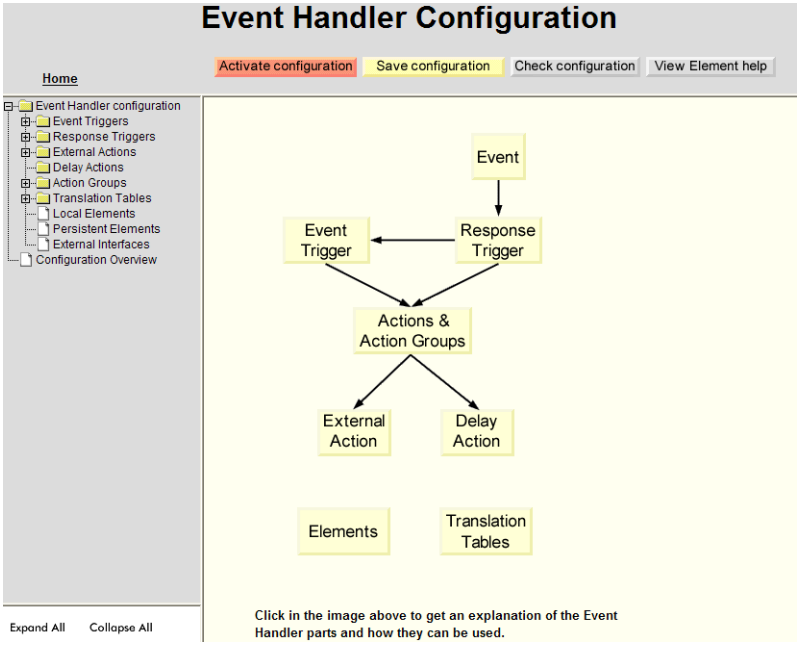


Figure 26. Event Handler Configuration

For simple configuration setup, it is only necessary to make configurations in External Actions and Assignments in the selected external action, and in Translation Tables > Location description.

It is possible to get explanation and instruction of the Event Handler parts by clicking on each of the boxes in the figure that shows the event flow.

Configuration Examples

You can find an example of a complete configuration that can be used as a template, in each type of External Action.

Event Triggers

This is where conditions on incoming events are defined, and where to activate predefined actions. There are different way of doing this, condition can be set up in Match Condition or in Activation. Several conditions can be set up for the Event that occur.

- Click ''Event Triggers'' and select trigger.

If no configuration is done it will trigger on all incoming messages.

- Match Conditions: if there exists more than one trigger and they should differ from each other the state and condition of the trigger can be changed.

It will activate the Extract and send data by default if nothing is done.

- Activations: conditions can be set on activation.

It will activate Extract and send data by default if nothing is done.

External Actions

This is where to create event element assignments.

- Open the folders, External Action > Extract and send data.
- Click Assignments, to create event element assignments.
- Define alarm type and location. There are four predefined examples:
- Alarm Type
- Alarm Type description
- Location
- Location description

Conversion tables

This is where to create and edit translation tables.

4.11.5 Alarm Management Client (AMC) Management

An external action on an event configured in Event Handler, can be to present information on an AMC (Alarm Management Client).

Communication between Unite CM and AMC

The Unite CM controls all communication with the presentation clients (AMC). The Event Handler has to be configured to send information to the client and also to confirm actions taken in the AMC (acknowledge and reset of alarms).

When Event Handler sends a presentation block, Unite CM notifies the client that there are new information to display, and when an acknowledge or reset request is received from the client, it sends a presentation response block back to Event Handler. When Event Handler receives the response it sends an updated presentation and Unite CM notifies the client that there are new information to display.

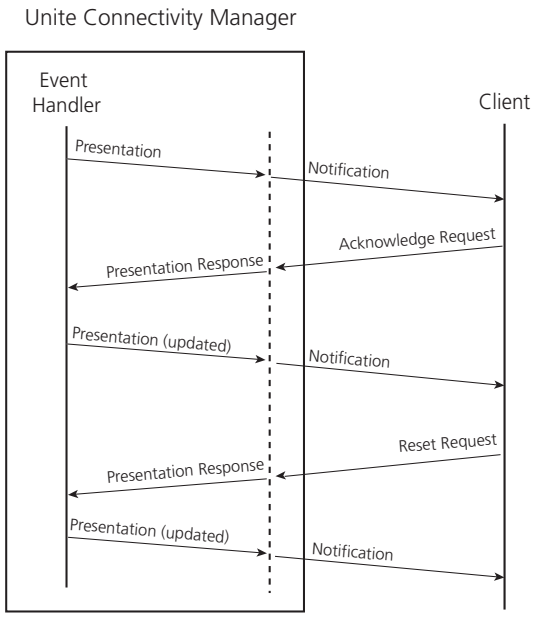


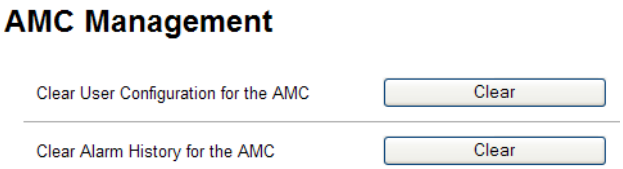
Figure 27. Example of the communication flow between Unite CM and an AMC

Clear User Configuration/Alarm History in the AMC

This AMC user configuration and alarm history can be cleared from the Unite CM.

1 Click ''Configuration'' on the start page.

2 Select Alarm & Events > Advanced Handling in the menu on the *Configuration* page.



3 Select ''AMC Management''.

4 Select if you want to clear ''user configuration'' or the ''alarm history'' in the AMC and click ''Clear'' on the same row.

4.11.6 Duty Assignment

Duty Assignment is where locations, in for example a hospital, and definitions of conditions for Event Elements are set up.

NOTE: Description of how to assign users to specific locations and associated events is found in a separate document. Refer to *User Manual, Duty Assignment in Unite Connectivity Manager, TD 92841EN*.

Figure 28. Duty Assignment in Unite Connectivity Manager

1 Click ''Duty Assignment'' on the start page. A Login window opens.

2 Enter User ID and Password and click ''OK''.

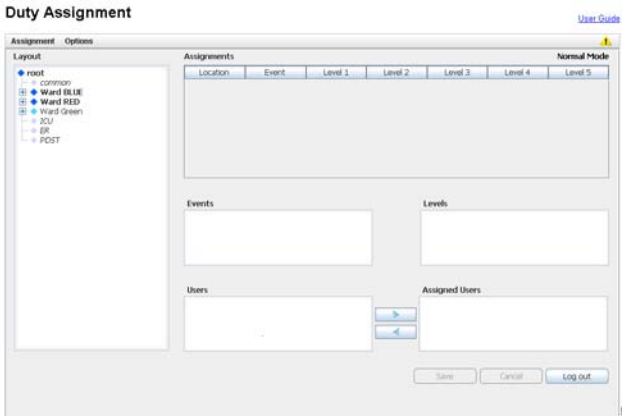


Figure 29. Duty Assignment page

4.11.7 Action Assignment

Events and actions and conditions for events, are configured here. The administration of access rights is also done in Action Assignment.

NOTE: Configuration work flow, definition of Event elements, Action configuration, Event assignments, and how to set up Access rights and Conversion tables are described in a separate document. Refer to *User Manual, Action Assignment in Unite Connectivity Manager, TD 92842EN*.

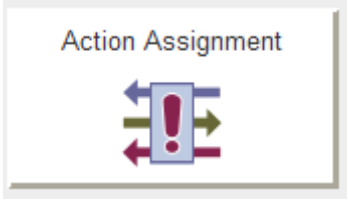


Figure 30. Action Assignment in Connectivity Manager

The first time, or when new Event and Actions are going to be implemented, Event and Actions has to be set up in a certain order.

1 Click ''Action Assignment'' on the start page.

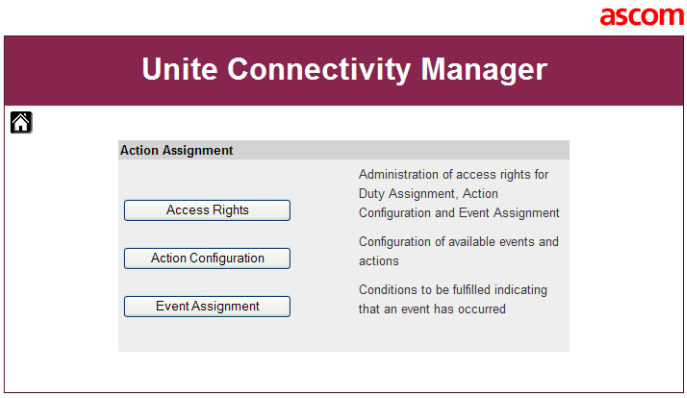

ascom
Unite Connectivity Manager
Action Assignment
Access Rights
Administration of access rights for Duty Assignment, Action Configuration and Event Assignment
Action Configuration
Configuration of available events and actions
Event Assignment
Conditions to be fulfilled indicating that an event has occurred

Figure 31. Action Assignment page

TIP: During the configuration there are many GUI's to log in to, and all of them prompt for User ID and Password. During the configuration it is possible to keep the main GUI applet open, that is, the first page that opens after you have logged in, in case you need to go back to make changes. It is only possible to log in to one GUI at the time, that is, if you already have one ''Action Configuration'' opened it is not possible to log in to another one.

4.12 System Supervision

Unite modules and other equipment in the system can be supervised, refer to 23 System Supervision and Security on page 180.

4.13 Status

4.13.1 Active Faults

Active Faults page is where the last 100 received active persistent fault logs are listed. For more information about the fault log, see 4.13.4 Fault Log on page 61.

1 Click ''Configuration'' on the start page.

2 Select Status > Active Faults in the menu on the *Configuration* page.

The following information is shown for each fault:

- Time when the fault occurred
- Level of the fault:
  - Critical error
  - Error
  - Warning
- Description of the fault, as defined in the module
- Type of module
- IP address and host name of the module that generated the fault

By expanding the fault in the list, additional information about the fault is shown containing:

- Fault ID
  This is used to reference a persistent fault when it later is reset
- Fault code
- Description of the fault code

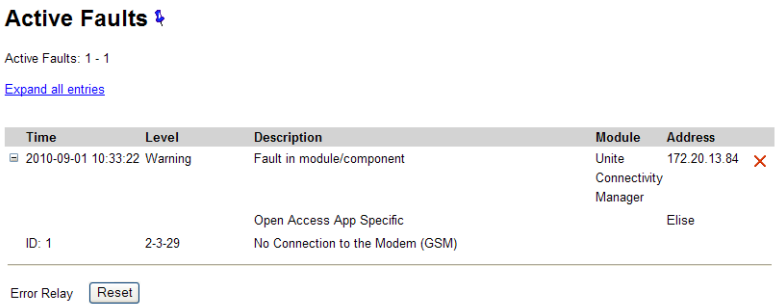


Figure 32. The Active Faults page

The fault will remain in the list until the module sends a status message confirming that the module is working properly again. It is also possible to delete the fault in the list by clicking the delete symbol.

NOTE: If the IP address or license is changed in Unite CM, the faults reported for the previous IP address/license will remain since no confirmation can be received. These faults must be manually deleted.

The active faults list page has to be manually updated by clicking the ''Update Page'' link uppermost on the page.

4.13.2 Reset the Error Relay

The error relay can be reset manually from the Active Faults page.

NOTE: When module redundancy is activated (see 4.14 Module Redundancy on page 65), the error relay should only be connected to the primary Unite CM since it is preferred to be the active module.

1 Click ''Configuration'' on the start page.

2 Select Status > Active Faults in the menu on the *Configuration* page.

3 Click ''Reset'' button.

4.13.3 Level of Seriousness for different Fault Types (Module Fault List)

A module fault list exists which shows codes and statuses etc. for each module in the system. The list is used for setting up actions in the fault handler for all errors of a certain level of seriousness.

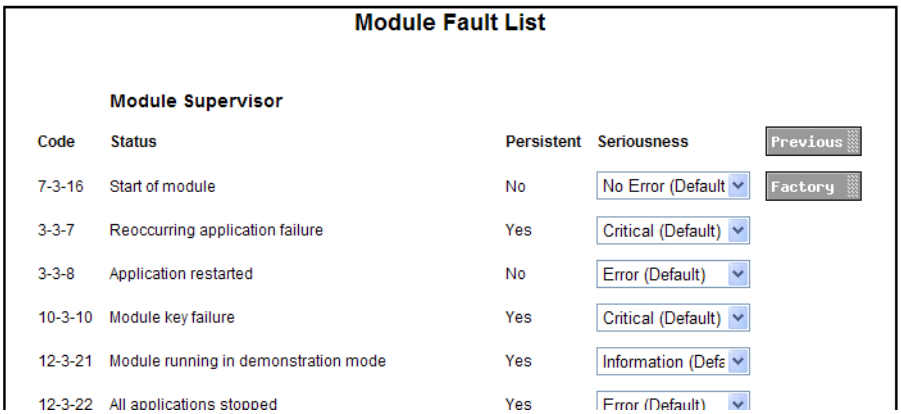
The level of seriousness can be changed for different fault types in the logs.

1 Click ''Configuration'' on the start page.

2 Select Other > Advanced Configuration in the menu on the *Configuration* page.

3 Click ''Troubleshoot'' button on the *Advanced Configuration* page.

4 Select ''Module Fault List'' in the menu to open the list.



5 Select level of seriousness in the drop-down list for the code(s) for which you want to change level.

4.13.4 Fault Log

The fault log in Unite CM is a centralized log file and shows a complete log of the faults in the system, on the assumption that other modules in the system are configured to send their fault logs to Unite CM. Every time a fault message is generated in the system, information about the fault is written to the log file. The maximum number of entries in the log file is 1050. When the log file is full, the 50 oldest entries are removed.

1 Click ''Configuration'' on the start page.

2 Select Status > Fault Log in the left menu on the *Configuration* page.

The first 25 log entries are shown. To get the following 25 log entries, click the ''Next'' link.

The following levels exist in the fault log:

- Information
- Individual reset
- All OK
- Critical error
- Error
- Warning

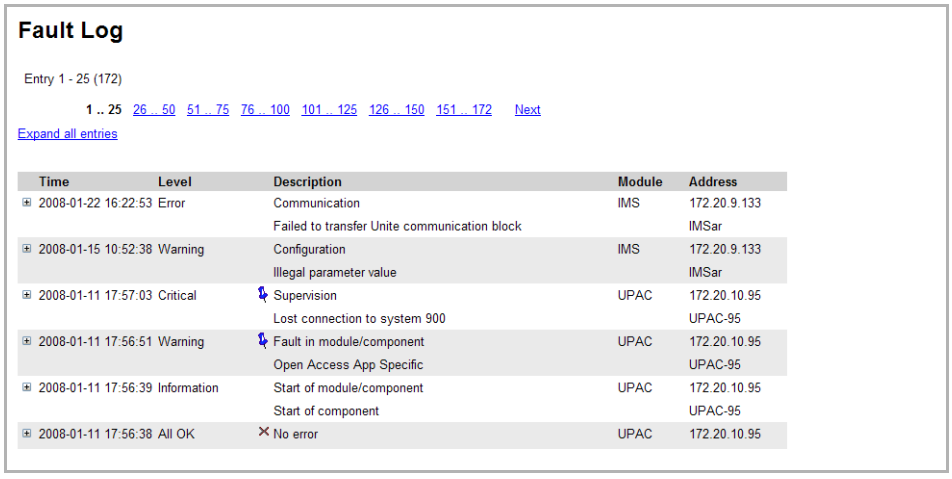

Fault Log
Entry 1 - 25 (172)
1 .. 25 26 .. 50 51 .. 75 76 .. 100 101 .. 125 126 .. 150 151 .. 172 Next
Expand all entries
Time Level Description Module Address
2008-01-22 16:22:53 Error Communication IMS 172.20.9.133
Failed to transfer Unite communication block IMSar
2008-01-15 10:52:38 Warning Configuration IMS 172.20.9.133
Illegal parameter value IMSar
2008-01-11 17:57:03 Critical Supervision UPAC 172.20.10.95
Lost connection to system 900 UPAC-95
2008-01-11 17:56:51 Warning Fault in module/component UPAC 172.20.10.95
Open Access App Specific UPAC-95
2008-01-11 17:56:39 Information Start of module/component UPAC 172.20.10.95
Start of component UPAC-95
2008-01-11 17:56:38 All OK No error UPAC 172.20.10.95

Figure 33. Example of a fault log in Unite CM.

Symbols used in the Fault Log

Symbol	Description
	Active persistent fault
	Persistent fault that has been handled
	Reset message, no fault exists

To get more detailed information about the events, it is possible to expand the log entries by clicking the ''Expand all entries'' link. Single log entries can be expanded by clicking the individual ''+'' symbol.

Block Repeated Faults

If a Status Log is received repeatedly, i.e. a Status Log with the same content and from the same Unite Address, it can be blocked for a set period of time. Repeated Status Logs can occur in the system for example if a Unite module sends Activity Logs to a Unite CM that has no license to handle Activity Logs.

Unite CM will discard all blocked Status Logs that are received during the set time, i.e. if the timeout is set to 10 minutes and the Status Log is received once every minute, every tenth Status Log will be stored in Unite CM. No actions will be executed for the discarded Status Logs.

Unite CM keeps track of up to 100 different Status Logs and the timeout is set individually for each one of them.

The timeout is set on the ''Administer Fault Log'' page, refer to 4.13.5 Administer Fault Log below.

4.13.5 Administer Fault Log

In the Administer Fault Log page, it is possible to export the log file to CSV (Comma Separated Values) file format and to clear the status log file from non-active faults. A timeout can be set to block repeated Status Logs i.e. the fault will be discarded and no actions will be executed.

1 Click ''Configuration'' on the start page.

2 Select Other > Administer Fault Log in the menu on the *Configuration* page.

Export Fault Log

1 Click ''Export''.

2 Click ''Save'' in the dialogue window and enter the file name (default name statuslog.csv) and the file path.

Clear Fault Log

1 Click ''Clear''.

2 Click ''Yes'' in the dialogue window to remove all non-active faults from the status log file.

Set Timeout

1 Enter the timeout in minutes (0-1000 minutes), the default value is 10 minutes.

If no Status Logs should be blocked, set the timeout to 0.

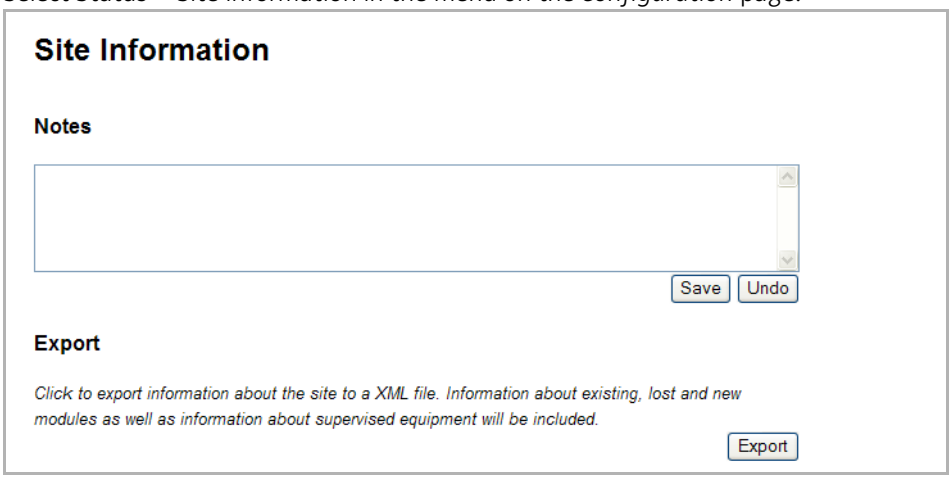
2 Click ''Set timeout'' to save the setting.

4.13.6 Site Information

In the Site Information page, it is possible to export information about the site to a text file. The text file can be used for support purposes. Information about the modules and the supervised equipment will be included in the text file as well as the last 100 status logs.

1 Click ''Configuration'' on the start page.

2 Select Status > Site Information in the menu on the *Configuration* page.


Site Information
Notes
Save
Undo
Export
Click to export information about the site to a XML file. Information about existing, lost and new modules as well as information about supervised equipment will be included.
Export

The Notes field can be used to describe the system. These notes will also be included in the exported site information. The exported file will be stored as an XML file.

4.13.7 WLAN Portables

To facilitate troubleshooting, the WLAN Portables page gives the possibility to list all handsets that are registered in the system.

View all Registered VoWiFi Handsets

1 Click ''Configuration'' on the start page.

2 Select WLAN Portables > List All, in the menu on the *Configuration* page.

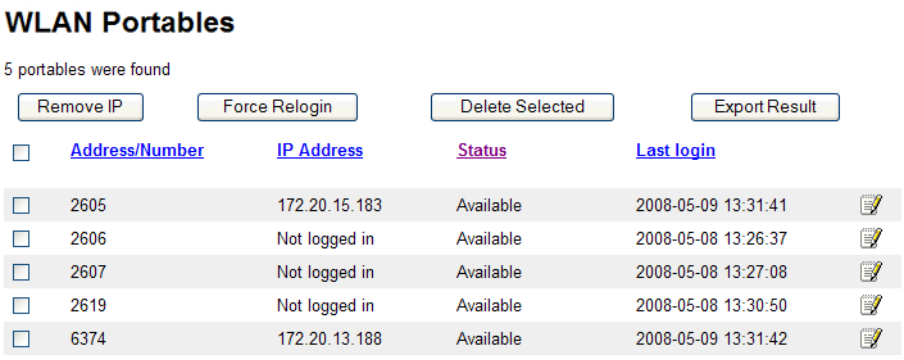


Figure 34. List with all registered VoWiFi Handsets

The list can be sorted by address/number, IP address, status or last login.

Save a List with all Registered VoWiFi handset

The list with all registered WLAN Portables can be exported to a comma separated file.

1 Click the ''Export Result'' button.

2 Select ''Save''. Enter a file name and the location where the file shall be stored and click ''Save''.

Remove IP Address, force a Relogin or Delete a VoWiFi handset

1 Select the handset(s) check box in the search result list, see Figure 29.

2 Click ''Remove IP Address'', ''Force Relogin'' or ''Delete Selected''.

• Remove IP Address

Can be used to refresh the address of a handset.

• Force Relogin

Can be used to check the connection with a handset.

• Delete Selected

Can be used to remove numbers not in use.

Show Details

Click the icon in the list, see figure 34 on page 63. All details of the chosen handset are viewed.

Figure 35. Handset details.

Change Absent Status

It is possible to change the Manual Absent status on the WLAN Portables pages.

1 View all VoWiFi handsets, refer to View all Registered VoWiFi Handsets on page 63.

2 Click the icon to view handset details, see Show Details above.

3 Select on/off in the Manual Absent drop-down list, see Figure 35.

NOTE: When absence is not set in the handset, that is offline[1], it is possible to let the Unite CM treat an offline handset as absent. See 15.4.3 Absence Status for Offline Devices on page 132 for more information.

1."Offline" means that the handset is out of range, turned off, or out of battery.

4.14 Module Redundancy

A redundant system consists of an active module and a standby module. When setting up the module redundancy in the system, the primary Unite CM will act as an active module, and the secondary Unite CM will act as a standby module. When the active module goes down, the system will automatically switch to the standby module that becomes an active module. The modules will indicate that the system no longer is redundant since no data synchronization between the modules can be performed.

Prerequisites

In order to set up module redundancy in Unite CM, the following requirements must be fulfilled:

- The hardware variant (Elise3 Lite *or* Elise3 Standard) must be identical on both the primary- and secondary module.
- The installed software version (4.xx or higher) must be identical on both modules.
- The Unite CMs must use the same type of SD card of minimum 1 GB capacity. Refer to Data Sheet, Unite Connectivity Manager, TD 92739EN for more information on which SD cards that currently are supported.
- The primary Unite CM must support module redundancy (license dependent feature).
- The secondary Unite CM must not have any licenses installed.
- RS232 Data Splitter. Only required if you want to connect equipment via serial interface (for example external equipment via TAP, ESPA or Line protocol).
- Three static IP-addresses. Ask your network administrator to obtain the IP-addresses. **TIP:** See also Prepare IP-addresses to be used in a redundant system (recommended).

Prepare IP-addresses to be used in a redundant system (recommended)

NOTE: It is assumed that your system already have one Unite CM installed and that an additional Unite CM will be installed in order to set up a redundant system.

The three static IP-addresses will be used as follows;

- two IP-addresses will be used by the primary- and secondary Unite CM
- the third IP-address will be used by the equipment (for example IP-DECT Base Stations, and VoWiFi handsets.) to interact with the active Unite CM when the system has become redundant. In this document, the third IP-address will be called "virtual IP-address".

To avoid changing the configured Unite IP-address in the equipment that will interact with the active Unite CM, follow the instructions below:

Network without DCHP Server

1 Replace the IP-address in the origin Unite CM with the static IP-address to be used by the primary module. The replaced IP-address can now be used as virtual IP-address by the external equipment.

2 Make sure the other Unite CM to be used as secondary module has been assigned correct IP-address.

Network with DCHP Server

1 Make sure that the origin IP-address of the Unite CM no longer is reserved to the Unite CM's MAC address. Note the IP-address still must be available but not reserved to a specific MAC address. Consult your network administrator. This IP-address will be used as virtual IP-address later on.

2 Ask your network administrator to reserve a new static IP-address to the origin Unite CM that later on will be used as primary module. The IP-address must be reserved to the module's MAC address.

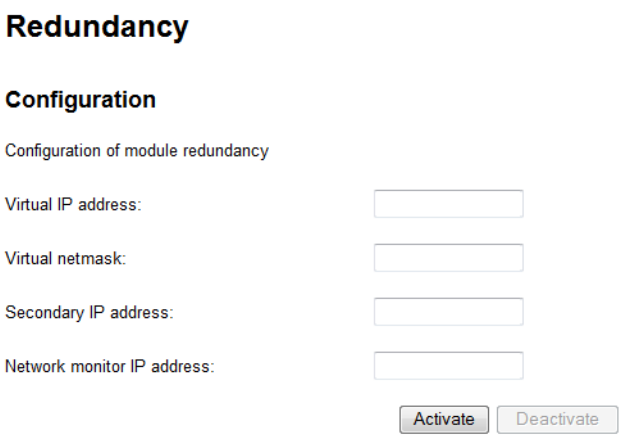
3 Ask your network administrator to reserve a static IP-address for the Unite CM to be used as secondary module. The IP-address must be reserved to the module's MAC address.

4.14.1 Configure Module Redundancy in Unite CM

Do the following on the Unite CM to be used as primary module:

1 Click "Configuration" on the start page.

2 Select Other > Redundancy on the *Configuration* page.



NOTE: Before proceeding, make sure that the SD memory cards are inserted in both modules.

3 In the *Virtual IP address* text field, enter the virtual IP-address.

4 In the *Virtual netmask* text field, enter the netmask of virtual IP-address.

5 In the *Secondary IP address* text field, enter the IP-address of the secondary Unite CM.

6 In the *Network monitor IP address* text field, enter the IP-address of the equipment to be used as network reference. The Unite CM will check that it has connection to the network by sending ICMP (Internet Control Message Protocol) ping inquiries to this equipment every second. If you do not want you use a network reference, set the IP-address to 127.0.0.1.

NOTE: The network topology used in the system may have impact on which equipment that should be used as network reference. See Appendix D.

7 Click "Activate".

NOTE: Once "Activate" is pressed, it is not possible to undo the activation of the module redundancy. However, it is possible to deactivate the module redundancy by clicking "Deactivate" and then click "Really deactivate". The module will reboot immediately. The GUI will not be updated automatically when the reboot is done. Update the GUI by clicking the "F5" button on your keyboard.

8 Click "Reboot now" or "reboot later".

The Unite CM will now reboot and copy data from its internal flash memory to the SD memory during the start up sequence. This can take up to 3 minutes. The GUI will not be updated automatically when the reboot is done. Update the GUI by clicking the "F5" button on your keyboard. Note that *Primary* will be stated in the GUI's upper left corner when the module is up and running again.

IMPORTANT: When the module redundancy has been activated, you must not remove the SD memory cards since the modules will use these as data storage instead of the internal flash memory. The Unite CM will continue to use the SD memory card as data storage even if the module redundancy is deactivated.

When the data has been copied, the primary Unite CM sends configuration settings to the secondary Unite CM that in turn reboots to apply the settings. After the reboot, the data will be synchronized with the secondary Unite CM's SD memory card. It can take up to one hour to synchronize all data to a SD memory card with 1 GB capacity the first time. During this time, the primary Unite CM is fully operational.

The LEDs on each Unite CM indicate the status of the synchronization.

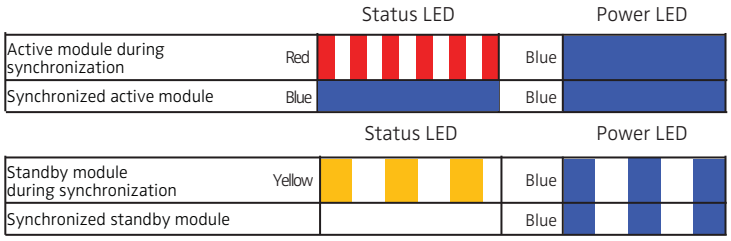


Figure 36. LEDs showing the status of synchronization.

It is also possible to view the synchronization status via the GUI, see Figure 37 and figure 38 on page 68. Use the virtual IP-address to access the active module and the static IP-address to access the standby module.

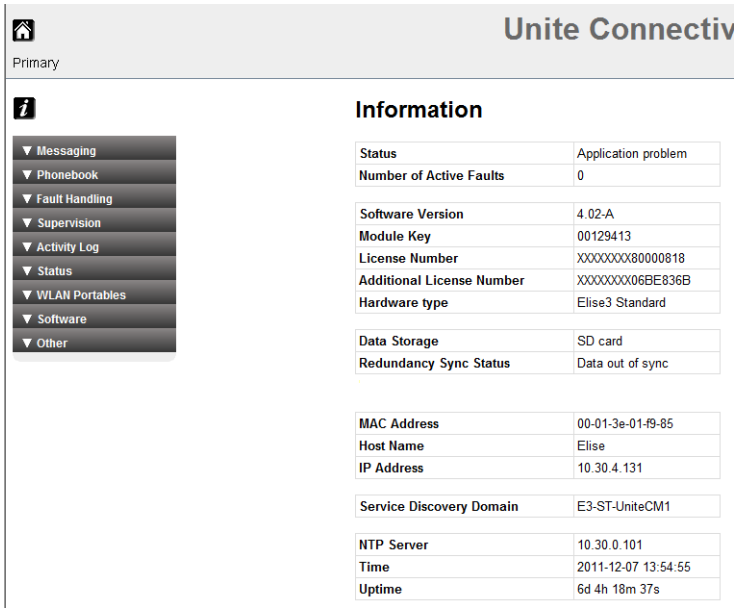


Figure 37. Status information shown on the primary module's Configuration page.

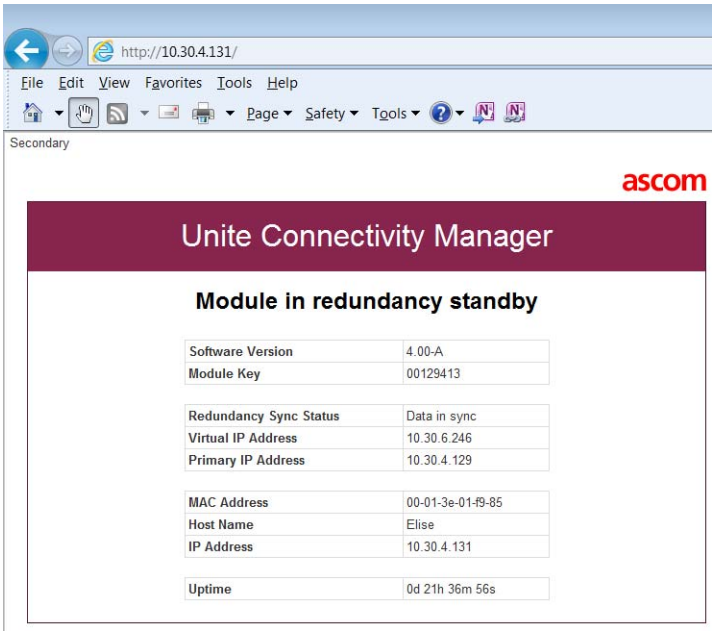


Figure 38. Status information shown on the secondary/standby module. Note that it is not possible to change any settings on a standby module.

In the *Redundancy Sync Status* field, the following status can be shown:

- Synchronizing - The synchronizing is in progress. Additionally, the amount of data (in percentage) that has been synchronized is also shown.
- Data in sync - The data in both modules are identical. The system is redundant when this status is shown.
- Data out of sync - The modules are not synchronized. This is shown for example if the connection to the other module is lost.

When the system has become redundant, the virtual IP-address will be used by the Unite CM that currently is active.

4.14.2 Connection of External Equipment via RS232 and S900 Interface

Connection of external equipment using RS232 serial interface or S900 interface must be connected physically to both Unite CMs. See B.6 R232 Cable Connections in a Redundant System on page 231, or C.1 System 900/A-bus Connections in a Redundant System on page 232 for more information.

4.14.3 Module Redundancy Test

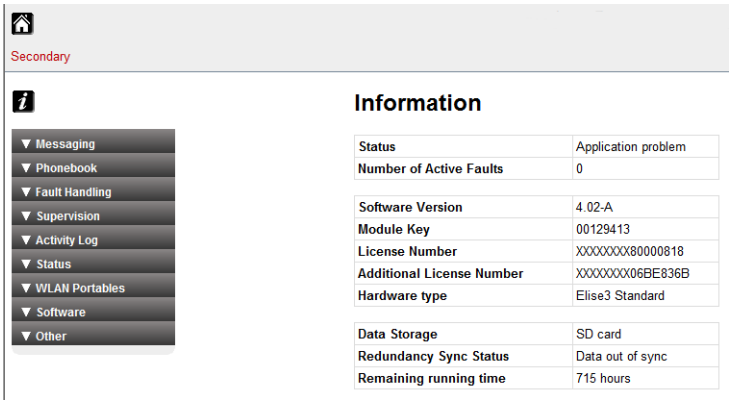
1 Unplug the active module's power cord from the power source.

The standby module will now start up to become an active module which takes up to 60 seconds before all applications are up and running.

The Status LED flashes (red) ■ ■ ■ indicating that the system no longer is redundant since the connection to the primary module (former active module) is lost.

When the standby module has become active, the Power LED changes to steady blue but the Status LED is unchanged as long the system is not redundant.

2 Enter the secondary module using the virtual IP-address. Note that *Secondary* is stated in the upper left corner indicating that this module currently is the active module.



3 Select Status > Active Faults on the *Configuration* page. The log shows for example that the secondary module is active and that the primary module has failed. Other faults might also be shown.

4 Perform an action to ensure that the active module works properly. For example send a message to a handset to check if it receives the message.

5 Connect the primary module and check if the secondary module starts to synchronize with the primary module. A completed synchronization is indicated as follows;

- On the secondary module; the Status LED and the Power LED will be steady blue as long the module acts as an active module.
- On the primary module; the Status LED is turned off and the Power LED will still flash blue as long the module acts as a standby module.
- The synchronization status on both modules will be changed to *Data in sync* when the data is synchronized.

After the test, it is recommended to switch back to the primary module again. See 4.14.5 Fallback to the Primary Unite CM on page 70.

NOTE: When switching between primary Unite CM and secondary Unite CM, it might take a while before devices appear in the Device Manager. The Online Status Time/Relogin Time determines the maximum time the devices have to relogin to the Device Manager. See 6 Device Configuration on page 74.

4.14.4 Restrictions on an Active Secondary Module

A secondary module that has become active, has redistricted functionality as follows:

- The secondary module can only be up and running as active module for 30 days without a repaired primary module connected. Note: If you for example shut down the secondary module day 10, it can still use the remaining twenty days when it is started again. If the repaired primary module is not connected within 30 days, the secondary module will fallback as a standby module.
- It is not possible to disable the module redundancy
- It is not possible to use the Troubleshoot mode
- It is not possible to perform a backup restore
- It is not possible to add a license
- It is not possible to run the Wizard
- It is not possible to activate the Demonstration Mode.

4.14.5 Fallback to the Primary Unite CM

When a secondary module has become an active module, it will only switch back to the primary module when the secondary module goes down. It is possible to manually switch back to the primary module when it is in standby mode after repair.

NOTE: If you for some reason reboot the secondary module via the GUI, the primary module will not take over as active module. However, if the secondary module is not up and running again after 3 minutes, the primary module will become active.

On the secondary module, do as follows:

1 Click ‘‘Configuration’’ on the start page.

2 Select Other > Redundancy on the *Configuration* page.

3 Click the "Fallback to primary module" button.

NOTE: It is only possible to press the button if the data has been synchronized with the primary module.

The primary module will now act as a active module and the secondary module will act as a standby module.

NOTE: When switching between primary Unite CM and secondary Unite CM, it might take a while before devices appear in the Device Manager. The Online Status Time/Relogin Time determines the maximum time the devices have to relogin to the Device Manager. See 6 Device Configuration on page 74.

4.14.6 Deactivate Module Redundancy

NOTE: This setting can only be performed on the primary module.

1 Click ‘‘Configuration’’ on the start page.

2 Select Other > Redundancy on the *Configuration* page.

3 Click the "Deactivate" button.

4 Select one of the following:

- Click "Cancel deactivate" to undo the deactivation.
- Click "Really deactive" to perform the deactivation. Both Unite CMs will now reboot immediately. The GUI will not be updated automatically when the reboot is done. Update the GUI by clicking the "F5" button on your keyboard.

5 Do one of the following:

- If the IP-address was changed in the modules: Change the IP-address in the former primary Unite CM to its origin IP-address. NOTE: If DCHP server is used, ask your network administrator to reserve the IP-address to the module’s MAC address.
- If the Unite CM’s IP-address was changed in the equipment (for example IP-DECT base station) that communicates with the Unite CM, change back to the Unite CM’s origin IP-address.

IMPORTANT: Do not remove the SD memory card from the Unite CM that acted as primary module. The SD memory card on that module will still be used as storage even when the module redundancy has been deactivated.

4.15 Back up the Configuration

The complete configuration for the current software on the module is included in the backup. Files that have been added or changed on the ftp-area are also included in the backup.

The backup file is saved in a proprietary file format and cannot be edited. Save it in a place where you can easily find it for a restore.

1 Click ''Configuration'' on the start page.

2 Select Other > Backup/Restore on the *Configuration* page.

3 Click the ''Backup'' button.

4 Click the ''Save'' button in the opened dialog.

5 Select a location and enter a file name, then save the file.

NOTE: Saving file can take several minutes if configuration contains many files, for instance if many software files and devices has been added to device management.

4.16 Restore the Configuration

NOTE: When Unite CM is restored, all changes that have been made since the last backup will be discarded.

1 Click ''Configuration'' on the start page.

2 Select Other > Backup/Restore on the *Configuration* page.

3 Click ''Browse'' button and select the backup file.

4 Click the ''Restore'' button.

The text ''Backup successfully restored!'' will be displayed and inform you when the restore is ready. Restoring can take several minutes if backup file is large, for instance if many software files and devices is included in backup.

5 Click the ''Restart Now'' or the ''Restart Later'' button. If the IP address or DECT interface has been changed the module needs to be restarted for the settings to take effect.

A restart will take a couple of minutes and during that time Unite CM is unreachable. When the restart is completed, the window will refresh to the Configuration page overview.

4.17 Selection of Data Storage

It is possible to select if configurations and data are to be stored on an external SD memory card instead of storing the information on the Unite CM's internal flash memory. The SD memory card can be used if higher storage capacity is needed. For information about which SD memory cards that currently are supported, see Data Sheet, Unite Connectivity Manager TD 92679GB.

IMPORTANT: Once SD memory card is selected as data storage, the Unite CM will use the SD memory card permanently. This means that it is not possible to roll back to the internal flash memory later on.

1 Click ''Configuration'' on the start page.

2 Select Other > Data Storage on the *Configuration* page.

3 Click "Activate".

5 Device Manager

The management of devices, such as handsets and chargers, are done in the Device Manager application in Unite CM.

NOTE: Make sure that the Device Manager is configured to communicate with the interface (for example IP-DECT) the devices are connected to. If not, the devices will not appear in the Device Manager. See 6.1 Device Management Setup on page 74.

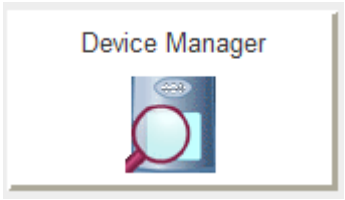
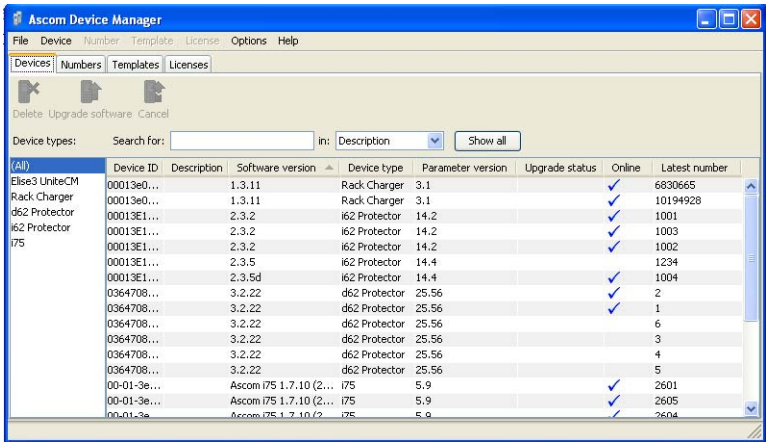


Figure 39. Device Manager in Unite CM.

1 Click ''Device Manager'' on the start page. A Login window opens.

2 Enter User ID and Password and click ''OK''.


Ascom Device Manager
File Device Number Template License Options Help
Devices Numbers Templates Licenses
Delete Upgrade software Cancel
Device types: Search for: in: Description Show all
(All)
Elise3 UniteCM
Rack Charger
d62 Protector
i62 Protector
i75
Device ID Description Software version Device type Parameter version Upgrade status Online Latest number
00013e0... 1.3.11 Rack Charger 3.1 6830665
00013e0... 1.3.11 Rack Charger 3.1 10194928
00013E1... 2.3.2 i62 Protector 14.2 1001
00013E1... 2.3.2 i62 Protector 14.2 1003
00013E1... 2.3.2 i62 Protector 14.2 1002
00013E1... 2.3.5 i62 Protector 14.4 1234
00013E1... 2.3.5d i62 Protector 14.4 1004
0364708... 3.2.22 d62 Protector 25.56 2
0364708... 3.2.22 d62 Protector 25.56 1
0364708... 3.2.22 d62 Protector 25.56 6
0364708... 3.2.22 d62 Protector 25.56 3
0364708... 3.2.22 d62 Protector 25.56 4
0364708... 3.2.22 d62 Protector 25.56 5
00-01-3e... Ascom i75 1.7.10 (2... i75 5.9 2601
00-01-3e... Ascom i75 1.7.10 (2... i75 5.9 2605

A description of Device Manager and how it is intended to be used, is found in a separate document; the User Manual, Device Manager in Unite Connectivity Manager, TD 92855EN.

6 Device Configuration

6.1 Device Management Setup

This setting determines which Device Handler interface the devices shall logon to. The Device Manager will then ask the interface for logged in devices, meaning that the devices will appear in the Device Manager.

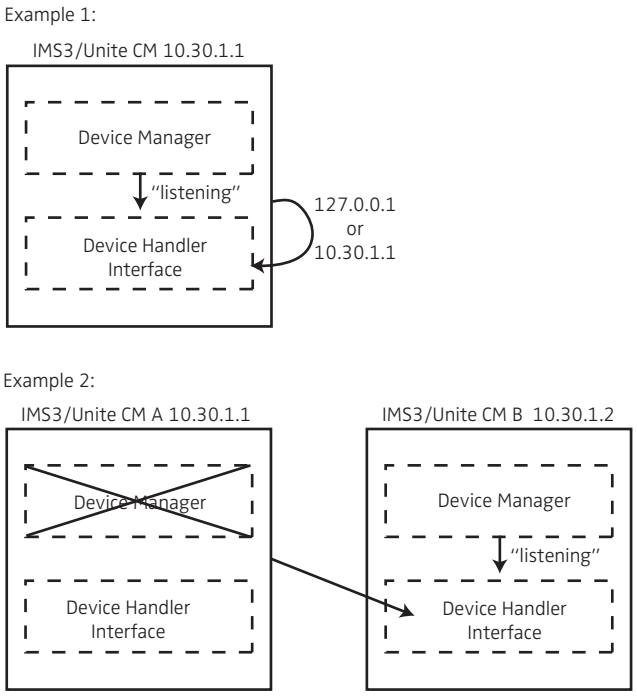


Figure 40. Device Handler Interface

Example 1:

The Unite module has a Device Manager enabled. In this case points the Unite module to its local Device Handler interface meaning that the devices will logon to that interface. The Device Manager asks the interface for logged in devices that will appear in the Device Manager.

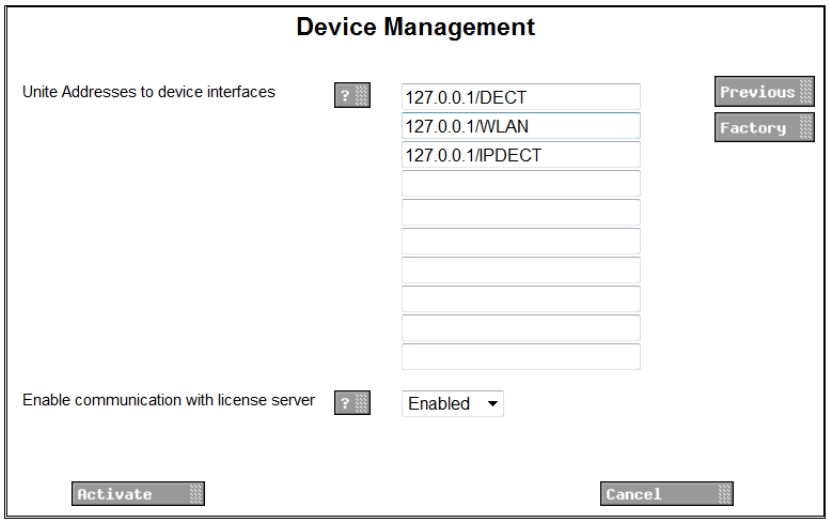
Example 2:

The Unite module A does not have a Device Manager enabled. In this case the Unite module A points to the Device Handler interface in Unite module B. All devices will logon to that interface, and the Device Manager will ask the interface about logged in devices that will appear in the Device Manager.

1 Click "Configuration" on the start page.

2 Select Other Settings > Advanced Configuration, on the *Configuration* page.

3 Click ''Device Management''. The Device Management page opens.



4 Enter IP address to the Unite module with the Device Handler interface the devices shall logon to, followed by the appropriate service.

- If IP-DECT handset is to be managed in the Device Manager, enter *<Unite IP address>*/DECT
- If IP-DECT Base Station is to be managed in the Device Manager, enter *<Unite IP address>*/IPDECT
- If WLAN handset is to be managed in the Device Manager, enter *<Unite IP address>*/WLAN

5 Set whether communication with the license server shall be enabled or not.

6 Click ''Activate''.

6.2 Device Handling Configuration

6.2.1 IP-DECT Handsets and Chargers

It is possible to set which device types that are allowed to log in to the module. This gives you the possibility to for example only allow handsets to log in to one Device Manager and chargers to log in to another Device Manager.

1 Click ''Configuration'' on the start page.

2 Select Other Settings > Advanced Configuration on the *Configuration* page.

3 Under DECT Interface, click ''Device Handling'' in the menu on the *Advanced Configuration* page.

4 Select the device type to enable/disable login from.

5 Change Status to desired value.

6 Click ''Activate''.

6.2.2 Fixed IP-DECT Devices

If your system having multiple Device Managers, it is possible to set which Device Manager the fixed IP-DECT devices (IP-DECT Base Station and IP-DECT Gateway) should logon to. This can be used to logon the fixed IP-DECT devices to one Device Manager while another Device Manager for example can be used for handsets.

The fixed IP-DECT devices can use either the Unite CM's IP-address or the Service Discovery Domain ID to logon to the wanted Device Manager. This chapter is only applicable when Service Discovery Domain ID is to be used.

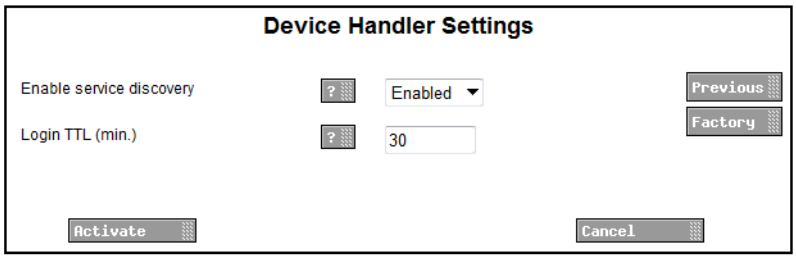
For example:

In the IP-DECT Base Station (IPBS), the Service Discovery is enabled with Domain ID set to "Unite_CM_1", and the Domain ID in your Unite CM is also set to "Unite_CM_1" (see 6.6 Service Discovery on page 77). In this case, enable the service discovery in your Unite CM in order to logon the IPBS to the Device Manager that matches the Domain ID.

1 Click ''Configuration'' on the start page.

2 Select Other Settings > Advanced Configuration on the *Configuration* page.

3 Under *IP-DECT Interface*, click ''Device Handling'' in the menu on the *Advanced Configuration* page.



4 In the *Enable service discovery* drop-down list, select "Enable" if the fixed IP-DECT devices use service discovery to find the Device Manager.

5 Click "Activate".

6.3 Online Status Report Time for Chargers

It is possible to set how often a device type must ''log in'' in order to be considered online. This is called ''Online Status Report Time''. To enable moving a charger without being logged out, it is possible to set a ''Status Log Delay Time''.

If the device has not logged in again within the Online Status Report Time, the Status Log Delay Time starts ticking. If the device does not log in again within that time a Status Report is sent to the Fault Log.

1 Click ''Configuration'' on the start page.

2 Select Other Settings > Advanced Configuration on the *Configuration* page.

3 Under DECT Interface, click ''Device Handling'' in the menu on the *Advanced Configuration* page.

4 Click the device type (that is, desktop charger or charging rack) to change settings for.

5 Enter On-line Status Report Time in minutes.

6 To set the margin, enter Status Log Delay Time in minutes.

7 Click ''Activate''.

6.4 Online Status Report Time for Handsets in a Charging Unit

It is possible to set how often a device type placed in a charging unit must ''log in'' in order to be considered on-line. This is called ''On-line Status Report Time''.

If the device has not logged in again within the On-line Status Report Time, it will be considered off-line.

1 Click ''Configuration'' on the start page.

2 Select Other Settings > Advanced Configuration on the *Configuration* page.

3 Under DECT Interface, click ''Device Handling'' in the menu on the *Advanced Configuration* page.

4 Select device type to change settings for.

5 Enter On-line Status Report Time in minutes.

6 Click ''Activate''.

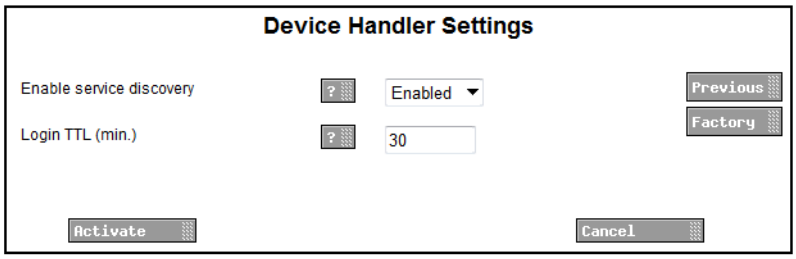
6.5 Online Status Report Time for Fixed IP-DECT Devices

It is possible to set how often fixed IP-DECT devices (IP-DECT Base Station and IP-DECT Gateway) must ''log on'' to the Device Manager in order to be considered online. If the fixed IP-DECT device has not logged in again within the Time to Live (TTL) time, it will be considered as logged out.

1 Click ''Configuration'' on the start page.

2 Select Other Settings > Advanced Configuration on the *Configuration* page.

3 Under IP-DECT Interface, click ''Device Handling'' in the menu on the *Advanced Configuration* page.



4 In the *Login TTL text* field, select the maximum time (10 - 1440 minutes) the fixed IP-DECT devices have to relogin before it will be considered logged out.

5 Click "Activate".

6.6 Service Discovery

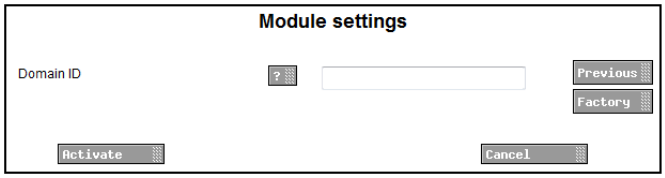
Service Discovery allows automatic detection of devices and services on a network without prior configuration. Unite CM and the devices that shall belong to that Unite CM have to be set to the same Domain ID.

1 Click ''Configuration'' on the start page.

2 Select Other Settings > Advanced Configuration on the Configuration page.

3 Under Other, click ''Service Discovery'' in the menu on the *Advanced Configuration* page.

4 In the Domain ID field, enter the Service Discovery Domain ID.



5 Click ''Activate''.

7 Additional System Settings

7.1 Mail Server Address

To be able to send e-mails the address to the Mail server needs to be specified. The address can also be set in the setup wizard.

1 Click ''Configuration'' on the start page.

2 Select Other > Advanced Configuration in the *Configuration* page.

3 Click ''Mail Server'' in the menu on the *Advanced Configuration* page.

4 Enter the IP address or hostname of the mail server and click ''Activate''.

NOTE: The company mail server must be set up to allow relaying to be able to send messages from the Ascom Messaging System as e-mails. (Contact your local IT department).

7.1.1 Hostname Setting in Fault Handler E-mail

The Unite CM can hide the hostname shown in the e-mails sent from a Fault Handler. This can be useful when a generic e-mail address should be shown. The hostname is included by default.

1 Click ''Configuration'' on the start page.

2 Select Other > Advanced Configuration in the menu on the *Configuration* page.

3 Click "Mail Server" on the *Advanced Configuration* page.

4 In the *Include hostname in outgoing faulthandler* mails drop-down list, select if the hostname should be included or not.

5 Click "Activate".

7.2 UNS/User Server

It is possible to set which number plan (that is UNS) to be used in a system. By default, the Unite CM is configured to use the local number plan, but it is possible to use another number plan by forwarding all application requests to another UNS. Additionally, it is also possible to forward to another UNS if the requested Call ID is not found in the local number plan (called multi-site number plan).

NOTE: The Unite CM does not support forwarding to an ESS.

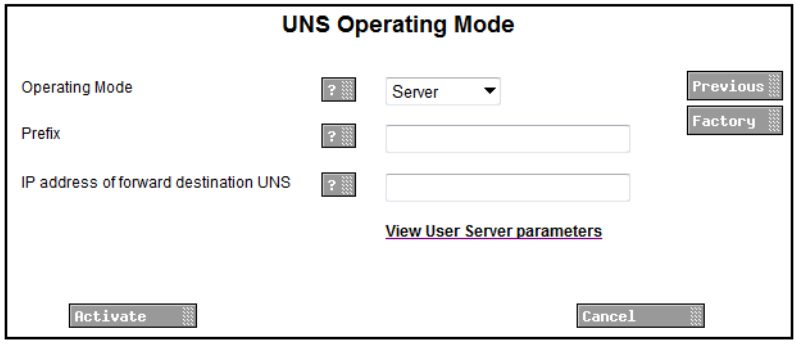
TIP: See also Function Description, Number Planning and Message Routing in Unite, TD 92254GB.

7.2.1 UNS Settings

1 Click ''Configuration'' on the start page.

2 Select Other > Advanced Configuration in the menu on the *Configuration* page.

3 Select "UNS" under *Other* on the *Advanced Configuration* page.



4 Select one of the following in the *Operating mode* drop-down list:

- Forwarding - Use if another number plan is to be used instead of the local number plan.
- Server - Use if only the local number plan is to be used (stand-alone), or if your system having a multi-site number plan meaning that the UNS can forward a request to another number plan if the Call ID is not found in the local number plan.

5 Prefix - Use if your system having a multi-site number plan. By adding a prefix[1] for each UNS, you can guarantee that each Call ID is unique in the entire multi-site number plan. NOTE: If you add a prefix for one UNS, all other UNSs in the system must also have a prefix.

6 Enter the IP address of the UNS that shall receive the requests in the *IP address of forwarding destination UNS* text field. NOTE: Leave empty if the UNS shall act as stand-alone module.

7 Click ''Activate''.

Continue and change the User Server settings if the *Operating Mode* was set to *Forwarding*.

7.2.2 User Server Settings

If the local number plan (UNS) should not be used, the Unite CM must forward the request to another User Server that holds the number plan.

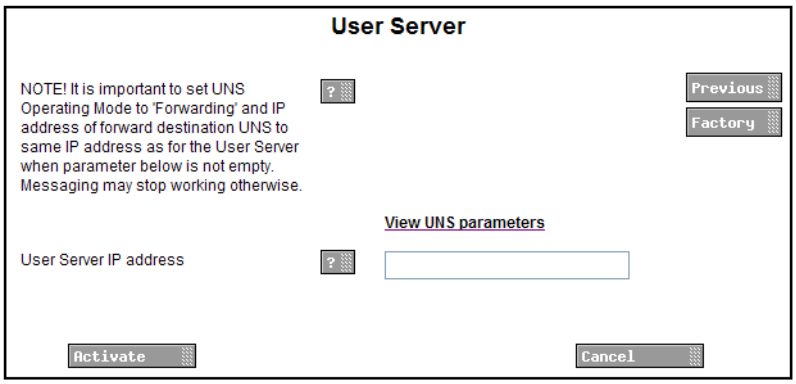
NOTE: This setting is only applicable if the *Operating Mode* is set to *Forwarding* (see 7.2.1 UNS Settings).

1 Click ''Configuration'' on the start page.

2 Select Other > Advanced Configuration in the menu on the *Configuration* page.

1.Any characters (max. 10) can be entered.

3 Click ''User Server'' under Other on the *Advanced Configuration* page.


User Server
NOTE! It is important to set UNS Operating Mode to 'Forwarding' and IP address of forward destination UNS to same IP address as for the User Server when parameter below is not empty. Messaging may stop working otherwise.
?
Previous
Factory
View UNS parameters
User Server IP address
?
Activate
Cancel

4 Enter the IP address of the User Server and click ''Activate''. The IP address must be the same as the IP address entered in *IP address of forwarding destination UNS* text field (7.2.1 UNS Settings).

7.3 Remote Service Center

A Remote Service Center makes it possible for a system supplier to monitor customer systems and give the customer instant support remotely if a fault occurs in the system.

Unite CM works as the gateway between Ascom products at a customer site and the Remote Service Center. Fault information and result from System Survey will then be sent to the Remote Service Center. Other modules in the system should be set up to send fault information to Unite CM. The communication between the customer site and the Remote Service Center will also be monitored. The default time is every 10 minutes.

If the communication towards Remote Service Center goes down, up to 1000 faults will be stored locally in Unite CM. When the communication is established again the non-transferred faults will then be transferred to Remote Service Center.

The parameter for blocking repeated faults also affects the faults that are transferred to Remote Service Center, refer to 4.13.5 Administer Fault Log on page 62.

7.3.1 Set up the Connection to the Remote Service Center

Only the credentials for the service when communicating with the Remote Service Center need to be entered to get the connection to work. The user name and password are automatically created when the customer site is created at the Remote Service Center.

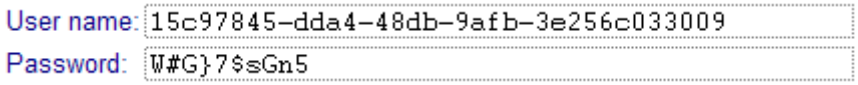


Figure 41. Example of automatically created credentials

1 Enter User name and Password in the text fields.

2 Click ''Activate''.

7.4 Remote Management

Through Unite CM, it is possible to establish a remote connection to a customer site. This makes it possible to configure and maintain sites, independent of distance.

The remote management connection is established via the Remote Management Client (RMC), which is a Windows based tool. For installation and configuration of the RMC, refer to Installation and Operation Manual, Remote Management Client, TD 92256GB.

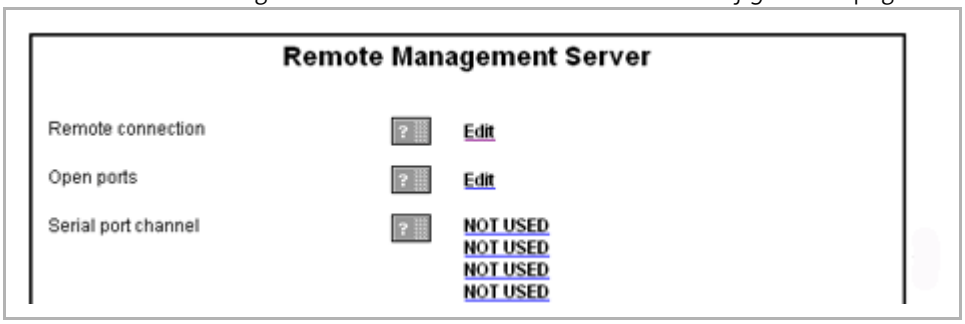
NOTE: Serial port 2 (COM2) on Unite CM is recommended to use for remote management.

To be able to connect remotely, the remote management server in Unite CM has to be configured. The helptext buttons in the GUI will give you more information about each parameter setting.

1 Click ''Configuration'' on the start page.

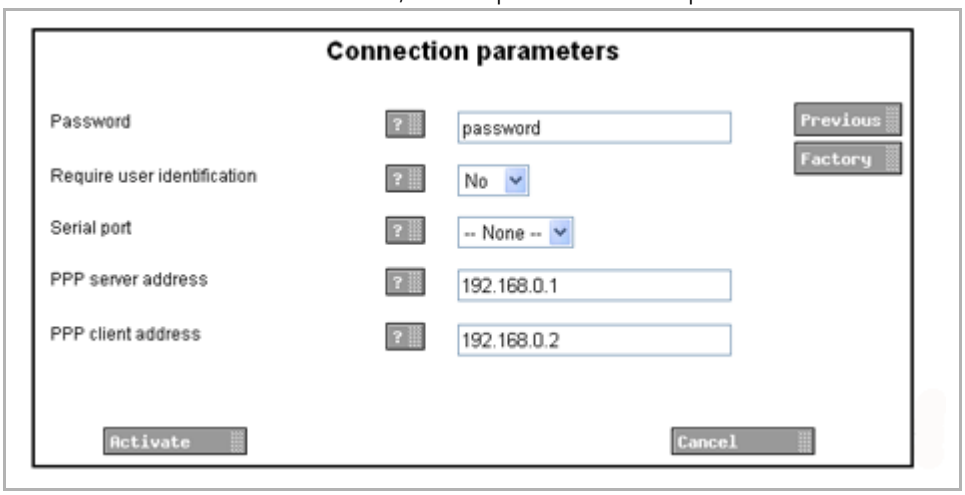
2 Select Other > Advanced Configuration in the menu on the *Configuration* page.

3 Select ''Remote Management'' in the menu on the *Advanced Configuration* page.



Remote connection

1 Click ''Edit'' for Remote Connection, to set up the connection parameters.

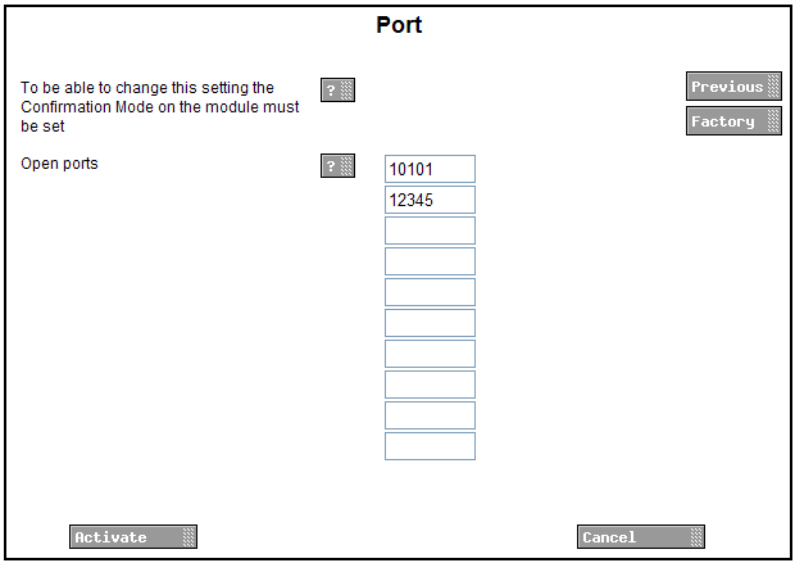


2 Set up the connection parameters and click ''Activate''.

Open ports

1 Click ''Edit'' for Open Ports in the Remote Management Server page, to open any additional ports that are needed for configuration tools.

This is a secured setting and before it can be activated it must manually be confirmed by pressing the mode button on the module.

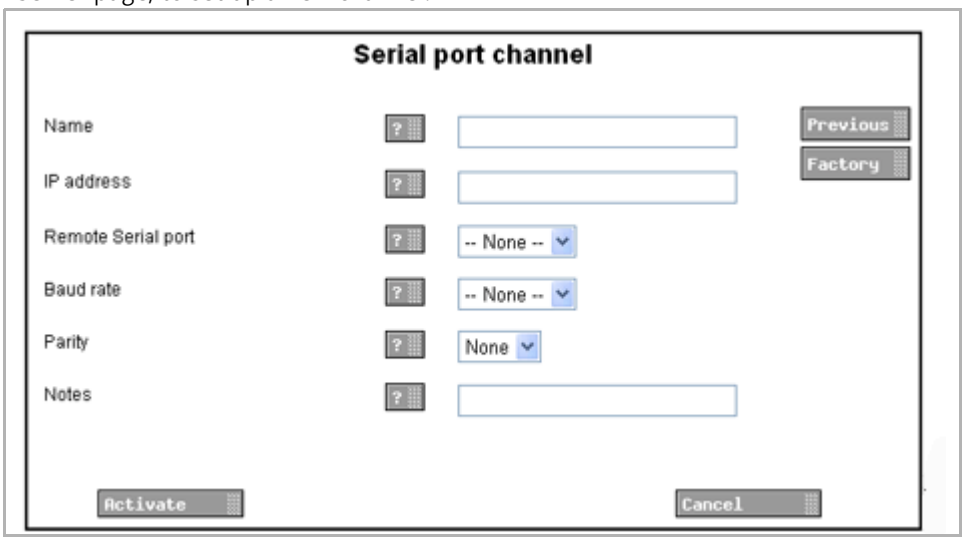


For WinBK, CSM and TIP port 10101 has to be open. To be able to use the Activity Log Viewer over a remote connection, port 10130 has to be open.

2 Set up the port parameters and click ''Activate''.

Serial port channel

1 Click one of the ''NOT USED'' links for Serial port channel in the Remote Management Server page, to set up a new channel.



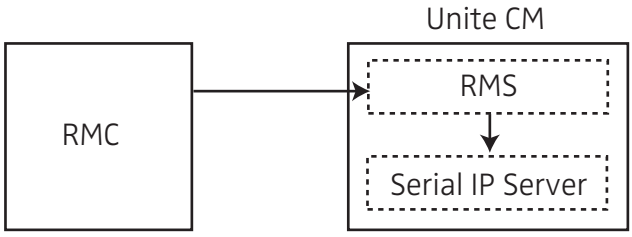
One serial port channel for each tool, for example WinBK for System 900 configuration, has to be set up. Web based configuration tools do not require serial port channels.

2 Set up the channel and click ''Activate''.

The configuration of the remote management server is described in detail in Function Description, Remote Management, TD 92257GB.

7.4.1 Serial IP Server Protocol

This parameter determines the version of Serial IP Server protocol to be used to establish a serial port channel from the RMC to the Serial IP Server. The Serial IP Server is a service that communicates with the Unite CM's COM-ports.



1 Click "Configuration" on the start page.

2 Select Other > Advanced Configuration in the menu on the *Configuration* page.

3 Select "Remote Management" in the menu on the *Advanced Configuration* page.

4 In the *Protocol Version* drop-down list, select one of the following:

- Select protocol version 1.0 if a legacy RMC is connected, or if a RMC is not connected through a VPN tunnel.
- Select protocol version 2.0 if a RMC is connected through a VPN tunnel. In this case RMC version 1.32 or later must be used.

7.5 Unlock GUI Managed by Unite AM

This option does only appear if the communication between Unite AM and Unite CM has been lost for more than 60 seconds. The option makes it possible to unlock the GUIs in the Unite CM that are managed by the Unite AM. If the communication is re-established, the GUIs in the Unite CM will be locked once again.

1 Click "Configuration" on the start page.

2 Select Other > Advanced Configuration in the menu on the *Configuration* page.

3 Select "UniteAM Management" in the menu on the *Advanced Configuration* page. An *UniteAM Handling* dialog window opens.

4 Click "Unlock" to unlock the GUIs in the Unite CM.

7.6 Open Access Protocol (OAP)

NOTE: OAPv4 requires an additional license.

This function makes it possible for client applications to communicate with other connected systems, for example the Cordless Telephone System. The protocol that is used for communication is called Open Access Protocol (OAP).

The OAP interface is defined by the OA-XML protocol. New services can be added by importing new OA-XML files, see 7.8 Importing new OA-XML file on page 86.

Refer to Function Description, Open Access Protocol (OAP), TD 92215GB for more information about the protocol and when it can be used.

New services can be added by importing new OA-XML files, see 7.8 Importing new OA-XML file on page 86.

7.6.1 Configuration

The Message Distribution lists for the different interfaces have to be configured to send the information (i.e. alarms, user data, location etc.) to the OAP Server in Unite CM, in order to give the client access to the information. The address of the OAP Server is xxx.xxx.xxx.xxx/OAP where "xxx.xxx.xxx.xxx" is the IP address of the Unite CM running the OAP Server application (usually internal host 127.0.0.1).

Refer to 15.3.3 DECT Message Distribution on page 130, 17.4 WLAN Message Distribution on page 138 and 18.2 System 900 Message Distribution on page 146.

7.7 Java Server/GSM

NOTE: Requires an additional license

Open Access Java makes it possible to communicate with an Ascom messaging system, as well as between an external application and an Ascom messaging system, by using a Java application. The Java application will run in an embedded environment and act as an interface between an external system and Ascom systems.

The Java interface is defined by the OA-XML protocol. New services can be added by importing new OA-XML files, see 7.8 Importing new OA-XML file on page 86.

The Unite CM is at delivery supplied with a preinstalled GSM/SMS application, but other applications can be developed and executed on the Unite CM, refer to *Programming Guide, Open Java Server (OJS), TD 92230GB*.

IMPORTANT: It is not possible to upload and run a java application on the Unite CM if the GSM interface is used.

7.7.1 Upload an Application to Unite CM

The application should be uploaded to the Unite CM FTP area.

1 Log on to Unite CM with an FTP client. Note that how to log on can differ between different FTP clients.[1]

Default username is "ftpuser" and default password is "changemetoo". xxx.xxx.xxx.xxx is the host name.

Examples:

- Windows Explorer: fill in "ftp://username:password@xxx.xxx.xxx.xxx" in the address field.
- Firefox: fill in "ftp://xxx.xxx.xxx.xxx" in the address field and log on with "username" and "password".

2 Upload the application to the Unite CM.

3 Restart the Java application from the Unite CM *Administration* page. The restart is accessed on http://xxx.xxx.xxx.xxx/apprestart (xxx.xxx.xxx.xxx is the IP address of the Unite CM). The user ftpuser can be used.

1.Internet Explorer is not an FTP client so its not possible to copy and move files from Internet Explorer.

4 Perform a functionality test of the uploaded application.

7.7.2 Configuration

The Message Distribution lists for the different interfaces have to be configured to send the information (i.e. alarms, user data, location etc.) to the Java Server in Unite CM, in order to give the client access to the information. The address of the Java Server is xxx.xxx.xxx.xxx/OAJ where ''xxx.xxx.xxx.xxx'' is the IP address of the Unite CM running the Java Server application (usually internal host 127.0.0.1).

Refer to 15.3.3 DECT Message Distribution on page 130, 17.4 WLAN Message Distribution on page 138 and 18.2 System 900 Message Distribution on page 146.

7.8 Importing new OA-XML file

It is possible to import new services, and update existing services, by importing a new OA-XML file to the Unite CM. The OA-XML description and OA-XML schema documents will also be updated when a new file is imported.

1 Click ''Configuration'' on the start page.

2 Select Other > Advanced Configuration in the menu on the *Configuration* page.

3 Select ''OA-XML'' in the menu on the *Advanced Configuration* page. The Import OA-XML file opens.

4 Click ''Browse'' and locate the file.

5 Click ''Submit File''.

New services are added to the OAP Interface/Java Server list on the System Information page. The Protocol version in the list shows the currently installed OA-XML version.

7.9 Logging

Logging information can be stored locally, but can also be distributed to other modules or applications. The System Activity Log can store ''activities'' such as messages, alarms, faults, input/output activities, etc. Activity logging is useful for troubleshooting.

1 Click ''Configuration'' on the start page.

2 Select Other > Advanced Configuration in the menu on the *Configuration* page.

3 Click ''Logging'' under Other, in the menu on the *Advanced Configuration* page.

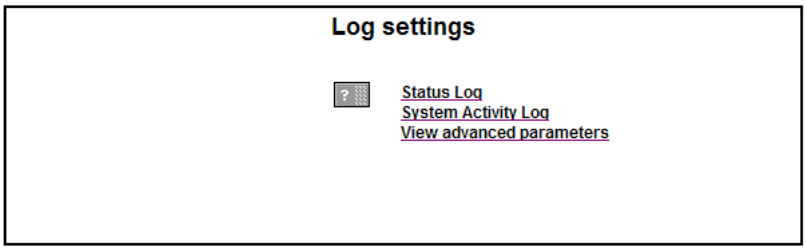


Figure 42. The Log settings page.

4 Click ''Status Log'', ''System Activity Log'' or ''View Advanced parameters''.

- Status Log and System Activity Log specifies the destinations for the logs.
- In View advanced parameters the time for the error relay to release in case of status log failure, is set. Here it is also possible to enable the Extended Activity

Log, which means that the start of an activity and any action between the start and stop, are also sent to the Log Viewer.

5 In the selected log page, enter settings.

6 Click ''Activate''.

7.10 Time Settings

It is possible to select where to fetch the time from, such as a web browser or a time server.

1 Click ''Configuration'' on the start page.

2 Select Other > Advanced Configuration in the menu on the *Configuration* page.

3 Click ''Settings'' under Time, in the menu on the *Advanced Configuration* page.

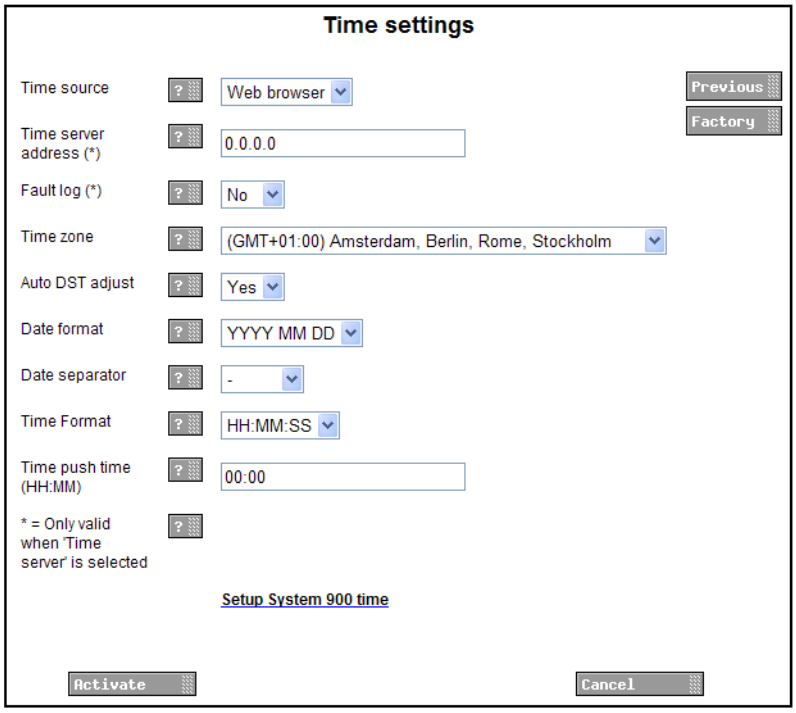


Figure 43. The Time Settings page.

4 The following settings can be selected/changed. Some of these parameters can also be set in the setup wizard:

Settings	Description
Time source:	Where to fetch the time; A-bus, web browser or NTP server
Time server address:	IP address to NTP server
Fault log:	Create fault log for time server faults
Time zone:	Current time zone
Auto DST adjust:	Automatic adjustment for daylight saving time
Date format:	Which date format to use
Date separator:	Which character to use to separate the date fields
Time Format:	Which time format to use
Time push time:	When to update all interfaces within the module

5 Click ''Activate''.

For additional information, see also Installation Guide, Elise3, TD 92679GB.

7.10.1 Set Time in System 900

The time in Unite CM can also determine the time in System 900.

1 Click the ''Setup System 900 time'' link in the Time settings window.

2 Select ''Yes''.

3 Click ''Activate''.

7.10.2 Manual Time setting (if Web browser is Time Source)

If Web browser has been selected as time source, the time must be set manually. Otherwise this setting shall not be done. The settings can also be set in the setup wizard.

1 Click ''Set time'' under Time.

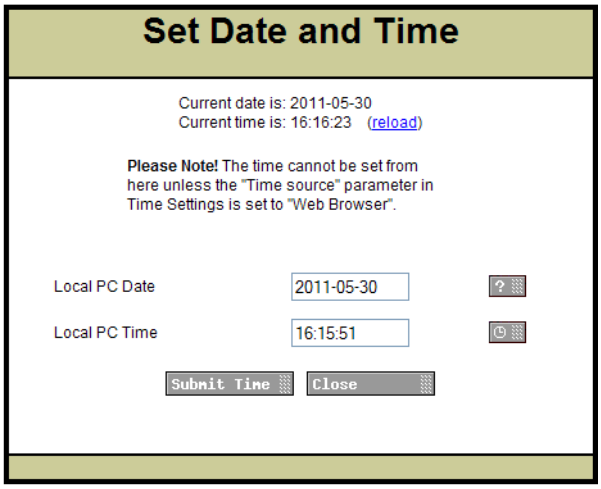

Set Date and Time
Current date is: 2011-05-30
Current time is: 16:16:23 (reload)
Please Note! The time cannot be set from here unless the "Time source" parameter in Time Settings is set to "Web Browser".
Local PC Date
2011-05-30
Local PC Time
16:15:51
Submit Time
Close

Figure 44. The Set Date and Time page.

2 Enter date and time.

3 Click ''Submit time''.

7.11 Network Setting

1 Click ''Configuration'' on the start page.

2 Select Other > Advanced Configuration in the menu on *Configuration* page.

3 Click ''Network'' under Common in the menu on the *Advanced Configuration* page.

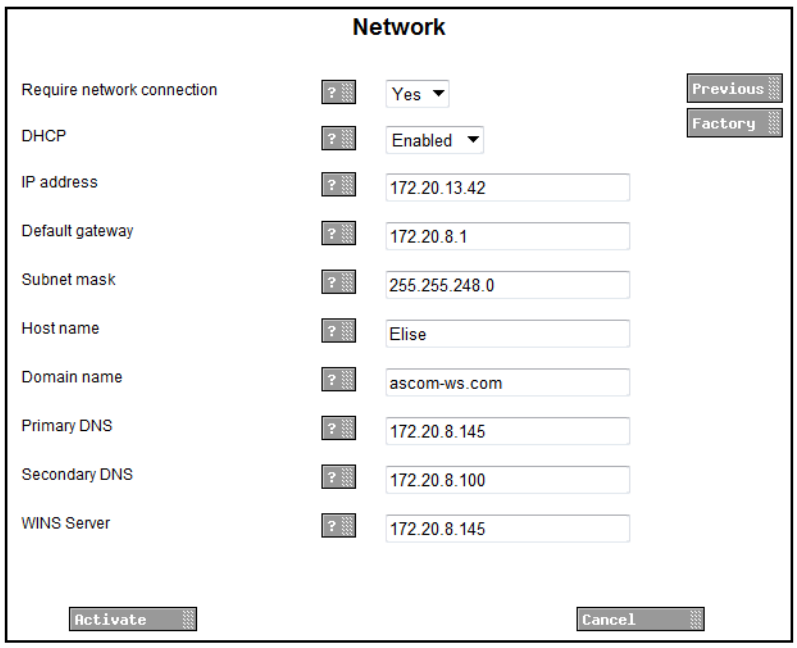


Figure 45. The Network page.

The following parameters can be set via the Advanced Configuration page. Some of these parameters can also be set in the setup wizard.

- Require network connection - Controls if the module needs a connection to the network to start up. This can be useful if you want configure the module before connecting it to a network.
- DHCP - Controls whether static or dynamic IP address shall be assigned to this Elise module. If DHCP is enabled, only the host name below is applicable.
- IP address - This parameter sets the IP address for Unite CM
- Default gateway - This parameter sets the IP address to a Gateway on the Local Area Network (LAN).
- Subnet mask - This parameter sets the network mask that is to be used. If this parameter is set to 0.0.0.0 it means that the Gateway never will be used.
- Host name
- Domain name - This parameter sets the desired domain name for Unite CM
- DNS Server - This parameter sets the IP address to a DNS if one exists. If no DNS Server is present on the network, set this parameter to 0.0.0.0.
- WINS Server - This parameter sets the IP address to a Primary WINS Server if one exists. If no WINS Server is present on the network, set this parameter to 0.0.0.0.

For additional information, see also Installation Guide, Elise3, TD 92679GB.

7.12 Setting License Number for Unite CM

It is possible to enter the license number via the Advanced Configuration page and the Setup Wizard. The Unite CM must reboot after the new license number has been entered.

TIP: If you upgrading your Unite CM with a license to increase the number of messaging users, you do not need to reboot the Unite CM. However, when changing the license via the Setup Wizard, you must always reboot the Unite CM.

NOTE: If your Unite CM shall support smart device users, you have to import a smart device license as described in 7.13 Import Smart Device License Document.

1 Click ''Configuration'' on the start page.

2 Select Other > Advanced Configuration in the menu on the *Configuration* page.

3 Click ''License'' under Common in the menu on the *Advanced Configuration* page.

4 Enter license number stated on the License certificate as follows:

- In the *License* field, enter the License Code 01 key
- In the *License 2* field, enter the License Code 11 key

NOTE: The other license fields are currently not in use.

5 Click ''Activate''.

7.13 Import Smart Device License Document

NOTE: This feature requires an OAP license.

The Unite CM can provide messages to smart device applications that in turn provide the messages to smart devices. It is possible to add smart device licenses by importing a license document in the form of a PDF file.

If this is done, the messaging user licenses will not be used for the smart devices since the smart devices have licenses dedicated just for them. The license document is provided by your supplier, or can be downloaded from the Extranet.

NOTE: The total number of users in Unite CM — that is, both messaging users and smart device users — cannot exceed 10 000 users.

1 Click ''Configuration'' on the start page.

2 Select Other > Advanced Configuration in the menu on the *Configuration* page.

3 Click ''Smart Device License'' under *Common* in the menu on the *Advanced Configuration* page. An *Upload smart device license file* dialog window opens.

4 Browse to the PDF file that contains the smart device license.

5 Click "Submit File".

After the license has been imported, you can manage the smart device users by following the instructions in 4.1 Add Users to Unite CM on page 20.

7.14 Reboot

Unite CM can be rebooted via the Advanced Configuration page.

1 Click ''Configuration'' on the start page.

2 Select Other > Advanced Configuration in the left menu in the *Configuration* page.

3 Click ''Reboot'' under Common in the menu on the *Advanced Configuration* page.

4 Click the ''Reboot'' button.

NOTE: If the Reboot page is reloaded, this will trigger another reboot.

8 Central Phonebook Configuration

This chapter describes the configuration of the Central Phonebook. For information about entering central phonebook entries, see 4.7 Manage Central Phonebook Entries on page 38.

The Central Phonebook gives the possibility to search for telephone numbers in a local database or in an LDAP server. If the search is to be forwarded to an LDAP or CMG server, the parameters need to be configured as described in 8.5 LDAP Parameter Setup on page 93 or 8.6 CMG Parameter Setup on page 95.

NOTE: If an LDAPv3 connection to a central phonebook is used, all settings needed are done in the setup wizard.

8.1 Technical Specification

The local database has defined limitations while most of the limitations for the LDAP/CMG server depends on the LDAP/CMG server used, see table below.

	Local Database	**LDAP/CMG Server**
Max. No. of phonebook entries:	500	Server dependent
Max. No. of characters in family name:	20	Server dependent
Max. No. of characters in first name:	20	Server dependent
Max. No. of digits in telephone number:	20	Server dependent
Max. No. of returned entries / request:	25	25
Handsets that can access the phonebook:[1]	Depends on handset type.	

8.2 Customize the Search Result Text

When a request is sent to the central phonebook, a text is included in the response that is sent to the handset. These texts can be customized, for example translated. The central phonebook supports search texts with character encoding UTF-8 (for example Russian characters and Swedish characters).

NOTE: These settings are not applicable for all handset types.

1 Click ‘‘Configuration’’ on the start page.

2 In the left menu, click Other > Advanced Configuration on the *Configuration* page.

1.See also documentation for the handset.

3 Click ''Phonebook'' in the menu on the *Advanced Configuration* page.

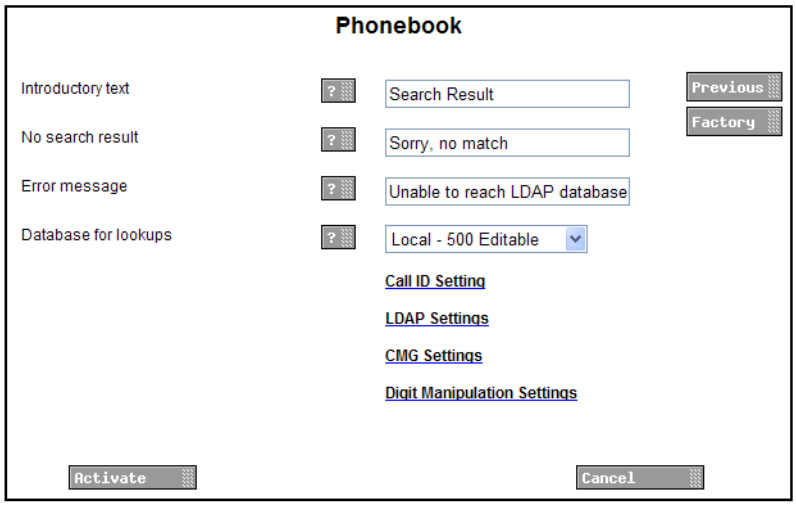


Figure 46. Central Phonebook Setup

4 Enter the texts that should be included in the search result, see table below for more information about the different texts and when they are used.

Default text	Description
Search result:	Included in a successful request before the entries that matched the request
Sorry, no match:	Sent when there were no match for the sent request.
Unable to reach LDAP database:	Sent after an unsuccessful query.

8.3 Central Phonebook Settings

It is possible to edit number and address to the central phonebook.

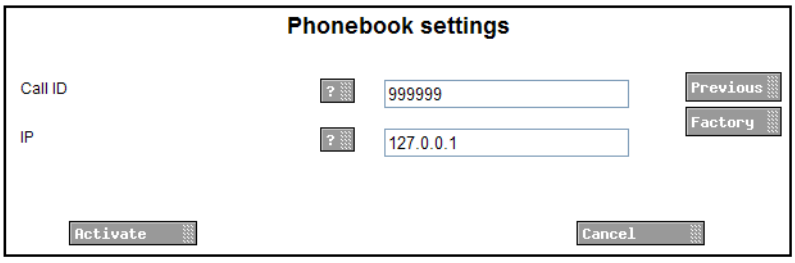


Figure 47. Phonebook Settings

1 Click ''Configuration'' on the start page.

2 In the left menu, click Other > Advanced Configuration on the *Configuration* page.

3 Click ''Phonebook'' in the menu on the *Advanced Configuration* page.

1 Click the Call ID Setting link.

2 Enter the number to the central phonebook in the Call ID text field (default 999999).

3 Enter the IP address to the module where the central phonebook is located (default localhost).

4 Click ''Activate''.

8.4 Select Central Phonebook Database

Select which database to use for telephone numbers; ''Local - 500 Editable'', ''Local - 2000 View only'', ''LDAP'', or ''CMG''.

- If the default local database is selected, continue in chapter 4.7.1 Import Entries to the Central Phonebook from a CSV File on page 38, 4.7.2 Export the Central Phonebook to a CSV File and 4.7.3 Add Entries to the Central Phonebook.
- If LDAP server is selected, continue in chapter 8.5 LDAP Parameter Setup on page 93.
- If CMG server is selected, continue in chapter 8.6 CMG Parameter Setup on page 95.

1 Click ''Configuration'' on the start page

2 Click Other > Advanced Configuration in the menu on the *Configuration* page.

3 Click ''Phonebook'' in the menu on the *Advanced Configuration* page.

4 Select which database to use in the ''Database for lookups'' drop-down list.

8.5 LDAP Parameter Setup

The Lightweight Directory Access Protocol version 3 (LDAPv3) is an application protocol for querying and modifying directory services running over TCP/IP. Unite CM starts an LDAP session by connecting to an LDAP server. Unite CM then sends operation requests to the server and the server sends responses in return.

An LDAP directory is a tree of directory entries and follows the structure below:

- An entry consists of a set of attributes.
- An attribute has a name and one or more values.

An entry can look like this:

dn: cn=John Ericson,dc=company,dc=com
cn: John Ericson
givenName: John
sn: Ericson
telephoneNumber: +1 888 555 6789

1 Click the LDAP settings link.

2 Enter the IP or hostname to the LDAP server in the LDAP Server or Proxy Address field.

3 Enter the port number used by the LDAP server in the Port Number field.

4 Select how to authenticate to the LDAP server in the Authentication Method drop down list.

NOTE: If the authentication method ''SASL/DIGEST-MD5'' is selected, the IP address for primary DNS server must be entered in the DNS server field on the Network setup page. Otherwise it is not possible to authenticate with the LDAP directory Microsoft Active Directory 2003.

5 Enter the user name used for logging on to the LDAP server in the User name field. It is a good idea to create a new user in the domain with access for the LDAP server.

6 Enter the password used for logging on to the LDAP server in the Password field.

7 Enter the user entries' parent DN in the Search Base DN field.
(The distinguished name for all users common entry.)

8 Enter the name of the attribute that holds the telephone numbers in the Number attribute field.

9 Select the appropriate option in the Type of Name Attribute(s) drop down list.

The option depends on if the name is stored in a single attribute or if it is split into two different attributes.

10 Enter name(s) of the attribute(s) containing first name and family name in the Name Attribute(s) field. If two attributes are used, enter the first name on the first line and the family name on the second line.

11 Enter an error message to be sent as an answer to a phonebook query that was unsuccessful, due to no answer from the server, in the Error message field.

8.5.1 Examples of Settings

- LDAP directory in VoIP Gateway

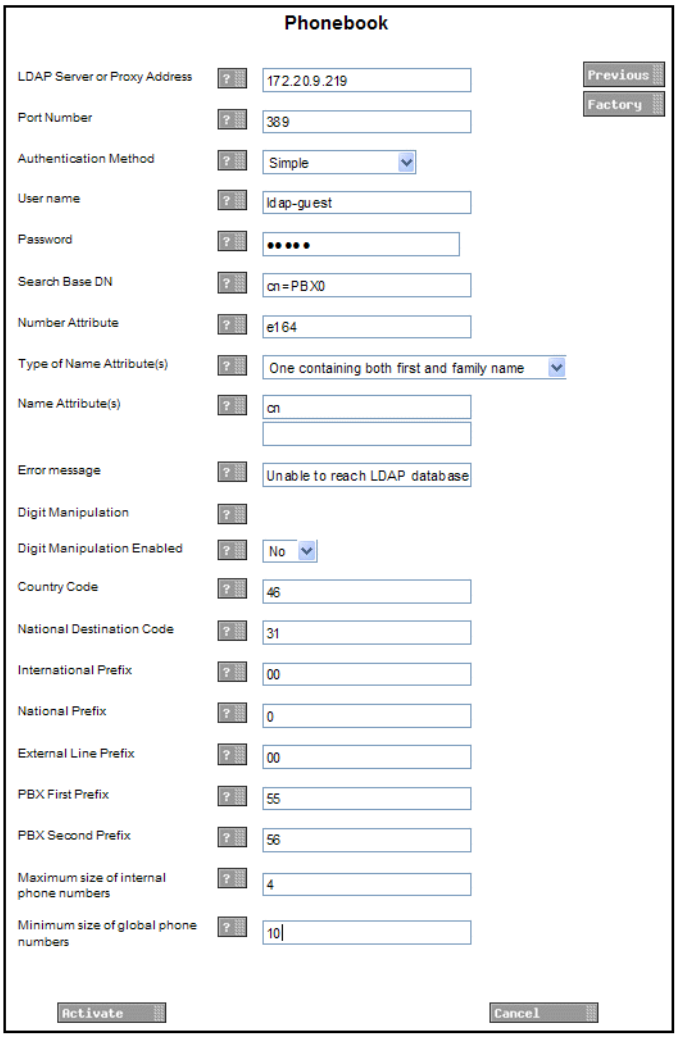


Figure 48. Settings for LDAP Directory in the VoIP Gateway

- Active directory 2003

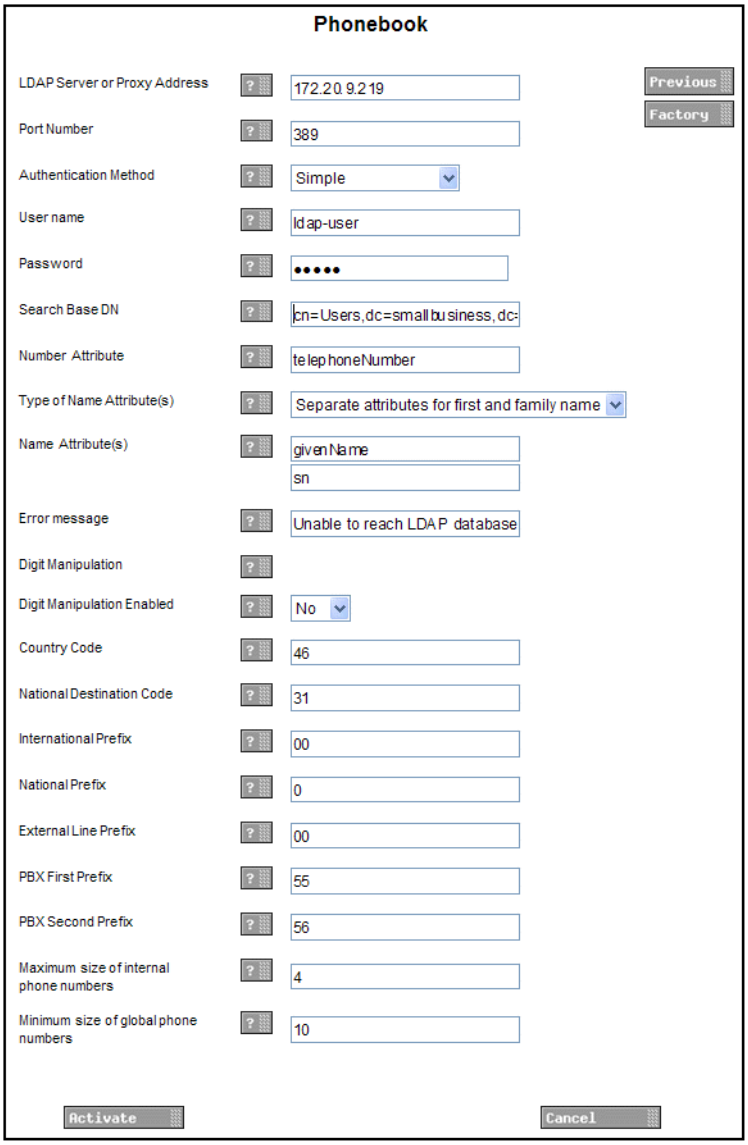
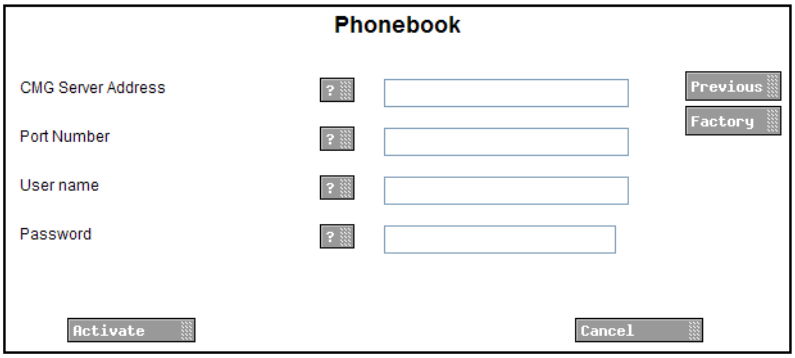


Figure 49. Settings for Active directory 2003

8.6 CMG Parameter Setup

The CMG is a central management server used for administration and it includes telephone directory services which can be used by Unite CM.



1 Enter the IP address or host name to the server in the *CMG Server Address* text field.

2 Enter the port number to be used by the CMG server in the *Port Number* text field.

3 Enter user name and password for logging in to the CMG server, in the *User name* and *Password* text fields.

4 Click ''Activate''.

8.7 Digit manipulation in the Central Phonebook

When importing telephone numbers, it is sometimes necessary to automatically change the way a number is written according to preset conditions.

Depending on where a number is situated, Unite CM can alter the number that is returned in a phonebook query. If, for example, the queried number is situated within the same local exchange, the telephone number is considered to be an internal number and the number is stripped from superfluous international prefixes, etc.

Telephone number standards

There are several standardized ways of writing telephone numbers.

The following formats are currently supported:

Format	Comment
+4631559300	E.164 international standard and E.123
(031)-559300	E.123 local number
+46(031)559300	National prefix + national destination code in parentheses
+46(0)31559300	National prefix in parentheses
+46(31)559300	Canonical address format
4631551234	Digits only. Conversion is controlled by setting maximum lengths of internal and national numbers.

Examples

The following figure shows the elements of a telephone number, +46(31)551234 (in canonical format), used in the parameter descriptions below.

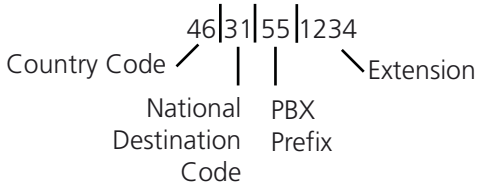


Figure 50. Example of how a telephone number is built up from different prefixes and extensions.

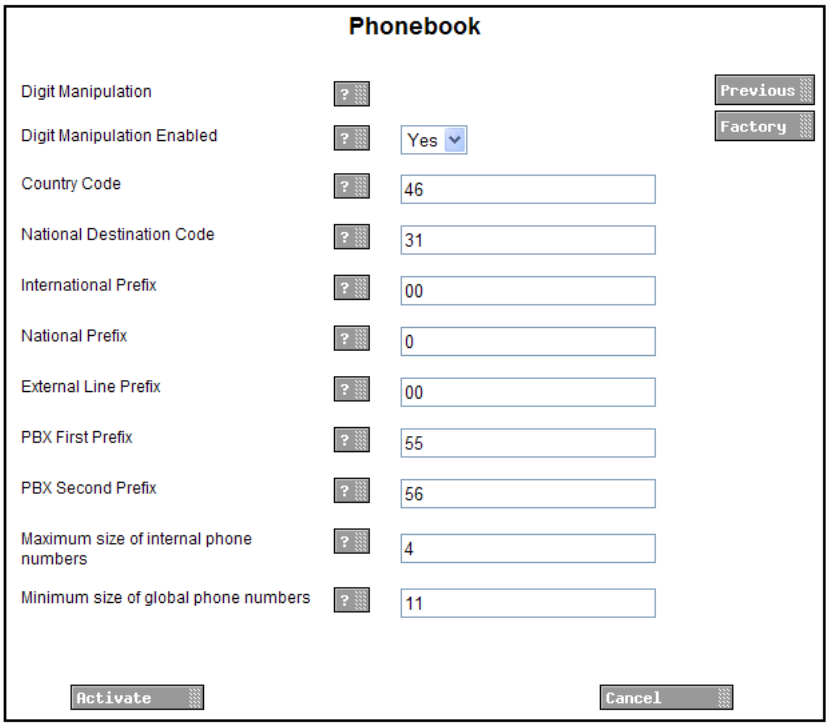


Figure 51. Example of digit manipulation settings.

The following examples illustrate how digit manipulation works in different queries. The queries are considered to be done from within +463155xxxx (local exchange), see also Figure 51 above.

- Example 1: The query is within the same local exchange.
  Queried number: 551234
  Digit manipulation identifies 55 as the local exchange prefix and strips 55 from the number.
  Resulting number: 1234
- Example 2: The query is within the same city (area code), but outside the local exchange.
  Queried number: 031612500
  Digit manipulation identifies 0 as National Prefix and 31 as National Destination Code, strips 031 from the number and adds 00 for external line.
  Resulting number: 00612500
- Example 3: The query is within the same country, but not in the same city.
  Queried number: 035158115
  Digit manipulation identifies 0 as National Prefix and 35 as National Destination Code and adds 00 for external line.
  Resulting number: 00035158115
- Example 4: The query is within another country.
  Queried number: +4781530555
  Digit manipulation identifies ''+47'' as an international call, skips the ''+'' and adds 00 for external line prefix and 00 for international prefix.
  Resulting number: 00004781530555

- Example 5: Size of internal number.

  Queried number: 1234

  Digit manipulation identifies that the number of digits in the telephone number is equal to the number of digits entered as ''maximum size of internal phone numbers''.

  Resulting number: 1234
- Example 6: Size of global number.

  Queried number: 47815305555

  Digit manipulation identifies that the number of digits in the telephone number is equal to the number of digits entered as ''minimum size of global phone numbers'', then adds 00 for external line prefix and 00 for international prefix.

  Resulting number: 000047815305555

Digit manipulation settings

The parameters for digit manipulation can be set via the Configuration page:

1 Click ''Configuration'' on the start page

2 Select Other > Advanced Configuration in the menu on the *Configuration* page.

3 Click ''Phonebook'' in the menu on the *Advanced Configuration* page.

4 Click the ''Digit Manipulation settings'' link on the Phonebook page.

The following parameters can be configured for digit manipulation:

- Digit Manipulation Enabled

  The digit manipulation function can be enabled and disabled. If the function is enabled, the parameters below apply, otherwise they do not apply.
- Country Code

  The Country Code is the prefix to be used when dialling to a particular country from another country. The country code is what follows after the + in a telephone number.

  The value is used to identify the country code in the number and remove it when it is not needed.
- National Destination Code

  The National Destination Code (NDC) is what follows after the country code in a telephone number.

  The value is used to identify the NDC in the telephone number and remove it when it is not needed.
- International Prefix

  The International Prefix is used to dial a call from a particular country to another country. This is followed by the country code for the destination country.

  This value is used to replace the + character when an international call is made.
- National Prefix

  National Prefix is used to make a call within a country from one city to another. The national prefix is followed by the national destination code for the destination of the call.

  This value is used for two purposes:

  - To identify the national prefix in the number and remove it when it is not needed.
  - To change a number when the destination is another city.
- External Line Prefix

  External Line Prefix is what needs to be dialled before the number to reach the public network.

  The value is used to change the telephone number if it is identified as an external number.

- PBX First Prefix

  PBX First Prefix is what precedes an internal number to create an external number.

  This value is used to compare with the phonebook number to decide whether the number is internal or external.
- PBX Second Prefix

  Points out an additional prefix to be handled in the same way as ''PBX First prefix''.
- Maximum size of internal telephone numbers

  Used for numbers that starts with a digit instead of ''+'' or ''(''. If the number is longer than this value, it is considered to be an external number.
- Minimum size of global telephone numbers

  Used for numbers that starts with a digit instead of ''+'' or ''(''. If the number is equal to or longer than this value, it is considered to be a global number.

9 Serial Interface In

NOTE: Included in Unite CM Compact license, but an additional license is required for the Unite CM Enterprise license.

The input serial interface makes it possible to receive pagings from external equipment and send them to handsets in the system. Note that the handset must be defined as a messaging user, refer to 4.1 Add Users to Unite CM on page 20.

The serial interface supports the ESPA 4.4.4 protocol and two ESPA dialects; the Ascom dialect (teleCOURIER) and Ericsson dialect with some limitations. The serial interface also supports the TAP 1.8 protocol and a simplified protocol called the Ascom Line protocol.

A detailed description of the two ESPA dialects and the Ascom Line protocol can be found in the document; Protocol, Serial Data Interface S942SI, TD 92088GB.

TAP (Telocator Alphanumeric Protocol) is a paging protocol used to transmit up to a thousand 7-bit characters to an alphanumeric pager.

For limitations in the three protocols, refer to Appendix J.

Cables for the connections are found in Appendix B: RS232 Connections on page 228.

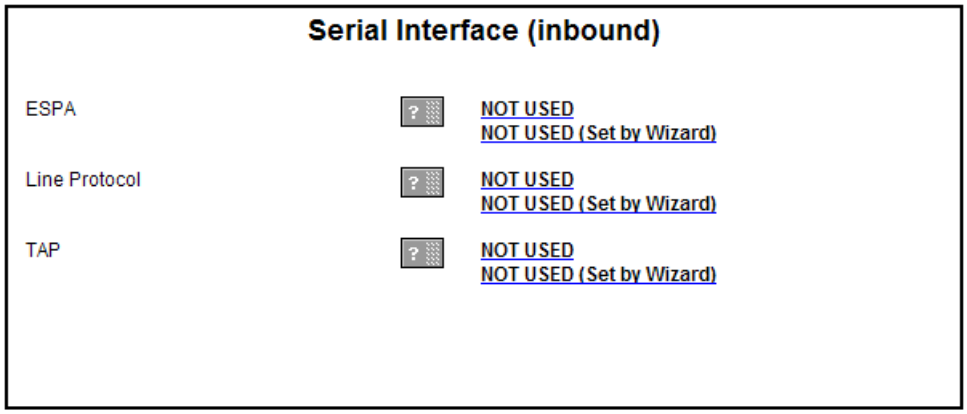
9.1 Serial Protocol Settings

Basic protocol settings are configured in the Setup Wizard. Detailed and more advanced settings can be configured from the Advanced Configuration page.

1 Click ''Configuration'' on the start page.

2 Select Other > Advanced Configuration in the menu on the *Configuration* page.

3 Select ''Serial Interface'' in the menu on the *Advanced Configuration* page.



4 Click a link for the protocol you want to use (ESPA, Line protocol or TAP) on the Serial Interface page.

5 Continue in 9.1.1 ESPA Protocol In, 9.1.2 Ascom Line Protocol or 9.1.3 TAP Protocol in on page 103.

9.1.1 ESPA Protocol In

1 The following settings can be selected/changed:

Settings	Description
Enabled:	Yes/No selection. Default: No
Name:	Description of the channel
Serial port:	Port selection (1,2) Default: None Port 2 will be selected when set from the Wizard, but both ports can be configured here. It is possible to have two ESPA systems connected to the Unite CM simultaneously, where one system is connected to port 1 and the other one is connected to port 2.
Bit rate:	Select bit rate. Default: 9600 bits/s.
Mode:	Select mode. Default: 8 Data bits, Even parity
Flow control:	Used for handshaking control. Default: None
ESPA dialect:	Select dialect, with or without an extra Carriage Return (CR). Default: TeleCourier extensions (i.e. Ascom dialect)
Control station selection:	Determines which module shall act as control station. Default: External equipment.
Address of external equipment:	Enter address (0 - 9). Default: 1
Address of this module:	Enter address (0 - 9). Default: 2
Default Call ID:	Number to call if not specified in the external equipment. Default: 000
IP Address of Event Handler:	A paging received via this serial interface will override the number plan and be sent directly to the Event Handler specified here.
Default display message:	Message to display if not specified in the external equipment. Default: BLANK
Default message priority:	Priority if not specified in the external equipment. Default: 7 (Normal)
Default beep code:	Beep code if not specified in the external equipment. Default: 2 beeps.
Default method for ack.:	Select how the paging shall be acknowledged if not specified by the external equipment. Default: No Ack.
Default urgency:	Urgency if not specified in the external equipment. Default: Normal.
Transmission delay (x10 ms):	How long to wait before transmission to external equipment. Default: 30 milliseconds
Identical pagings treatment:	How to handle identical pagings. Default: Not accepted.
Running number to ext equipment:	If running number shall be sent or not. Default: No

Timeout mode:	Determines when to start timeout mode i.e. remove paging from queue. Default: after ''Call Terminated'' call status.
Timeout mode TTL (seconds):	Determines the time for timeout mode i.e. during this time the paging remains in the queue after the ''Timeout mode'' has started. Default: 5 seconds.
Manual Ack type:	Dependent on if the external equipment supports negative acknowledge. Default: Positive and Negative manual acknowledge.
Manual Ack TTL (minutes):	How long a paging with manual acknowledge remains in the queue after transmission of Call Terminated call status. Default: 5 minutes.
Message Ref. ID TTL (minutes):	How long a Message Reference ID remains in queue. Only valid for Ascom dialect. Default: 5 minutes.
Interactive Message Option Text for Callback number: Note: For this setting to have effect, Interactive messaging (IM) must be supported by the handset.	Defines text that will be added to call digits sent from external equipment. The text and the number to call, is received as an option in the receiving handset. The call digits are dialled when the user selects the option. Max 40 characters. Note: Overrides Message Ref. ID TTL. Leave empty if data identifier 9 is used for message reference.
Return Status Information:	Defines if status information for ongoing pagings shall be sent back to external equipment. Set to ''No'' if external equipment have problems handling status information. Default: Yes.
Supervision time for communication (seconds):	Defines the time before lost communication with external equipment will be considered as a fault and sent as a Status log. If set to ''0'' no supervision is done. Max 3600 seconds Default: 0
ASCII conversion table:	Makes it possible to convert display message characters.

2 Click ''Activate''.

9.1.2 Ascom Line Protocol

1 The following settings can be selected/changed:

Settings	**Description**
Enabled:	Yes/No selection. Default: No
Name:	Description of the channel

Serial port:	Port selection (1,2) Default: None Port 2 will be selected when set from the Wizard, but both ports can be configured here. Note that only one port at the time can be used.
Bit rate:	Select bit rate. Default: 9600 bits/s
Mode:	Select mode. Default: 8 Data bits, Even parity
Flow control:	Used for handshaking control. Default: None
Default Call ID:	Number to call if not specified in the external equipment. Default: 000
IP Address of Event Handler:	A paging received via this serial interface will override the number plan and be sent directly to the Event Handler specified here.
Default display message:	Message to display if not specified in the external equipment. Default: BLANK
Default message priority:	Priority if not specified in the external equipment. Default: 7 (Normal)
Default beep code:	Beep code if not specified in the external equipment. Default: 2 beeps
Transmission delay (x10 ms):	How long to wait before transmission to external equipment. Default: 30 milliseconds
Status to ext equipment:	If status characters ACK/NAK shall be sent on protocol level to external equipment. Default: Yes
Start character :	Start character for the message. Default: < (3C Hex)
End character:	End character for the message. Default: > (3E Hex)
Record separator character:	Record separator character for the message. Default: / (2F Hex)
ACK character:	Character for positive acknowledge of the message on protocol level. Default: A (41 Hex)
NAK character:	Character for negative acknowledge of the message on protocol level. Default: N (4E Hex)
ASCII conversion table:	Makes it possible to convert display message characters.

2 Click ''Activate''.

9.1.3 TAP Protocol in

1 The following settings can be selected/changed:

Settings	**Description**
Enabled:	Yes/No selection. Default: No
Name:	Description of the channel

Serial port:	Port selection (1,2) Default: None Port 2 will be selected when set from the Wizard, but both ports can be configured here. Note that only one port at the time can be used.
Bit rate:	Select bit rate. Default: 9600 bits/s
Mode:	Select mode. Default: 8 Data bits, Even parity
Flow control:	Used for handshaking control. Default: None
Default Call ID:	Number to call if not specified in the external equipment. Default: 000
IP Address of Event Handler:	A paging received via this serial interface will override the number plan and be sent directly to the Event Handler specified here.
Default display message:	Message to display if not specified in the external equipment. Default: BLANK
Default message priority:	Priority if not specified in the external equipment. Default: 7 (Normal)
Default beep code:	Beep code if not specified in the external equipment. Default: 2 beeps
Default urgency:	If set to High ''Stand-by'' mode in receiver is broken through. Default: Normal.
Transmission delay (x10 ms): (Advanced)	How long to wait before transmission to receiver. Default: 30 milliseconds
Enable checksum validation: (Advanced)	Set to ''No'' if, for example, external equipment. uses an algorithm that differ from the 7-bit value used in TAP. Default: Yes
Delay time before a log on timeout occurs: (Advanced)	How long to wait before disconnecting the external equipment. Valid values: 0-127 where 0 means 'Not enabled'. Default 8 seconds
Delay time before a block timeout occurs: (Advanced)	How long this module shall wait before hanging up. Valid values: 0-127 where 0 means 'Not enabled'. Default 4 seconds.
Numbers of allowed times to log on: (Advanced)	How many log on attempts from external equipment shall be permitted. Valid values: 1-127. Default 3 tries.
Numbers of allowed checksum failures: (Advanced)	How many checksum failures from external equipment shall be permitted. Valid values: 1-127. Default 3 tries.
Numbers of allowed timeouts:	How many timeouts shall be permitted. Valid values: 1-127. Default 3 timeouts.
ASCII conversion table:	Makes it possible to convert display message characters.

2 Click ‘‘Activate’’.

10 Serial Interface Out

NOTE: Requires an additional license, see 1.1 Licenses for Unite CM on page 1.

The output serial interface makes it possible to send messages to external paging systems. The output serial interface supports the ESPA 4.4.4 protocol and the TAP 1.8 protocol. A description of cables for the connections are found in Appendix B: RS232 Connections on page 228.

10.1 Output Serial Protocol Settings

Settings are configured from the *Advanced Configuration* page.

1 Click "Configuration" on the start page.

2 Select Other > Advanced Configuration in the menu on the *Configuration* page.

3 Click a link for the protocol you want to use (ESPA Out or TAP Out) in the menu on the *Advanced Configuration* page.

4 Continue in 10.1.1 ESPA Protocol Out or 10.1.2 TAP Protocol Out.

10.1.1 ESPA Protocol Out

The following settings can be selected/changed:

Serial Communication

The parameters that can be set in the ESPA Serial Communication Settings page are:

Settings	Description
Enabled:	The communication can be enabled or disabled. If disabled, the serial port is free to use for other purposes. Default: No.
Serial port:	Port selection (1,2): Default: 2.
Baud Rate:	Select Baud rate. Default: 9600 bits/s.
Data Bits:	Number of data bits for this serial communication. Default: 8.
Stop Bits:	Number of stop bits for this serial communication. Default: 1.
Parity:	Parity to be used for this serial communication. Default: Even.
Hardware Flow Control:	Enables or disables hardware flow control. Default: Disabled.

ESPA Protocol

The parameters that can be set in the ESPA Protocol Settings page are:

Settings	Description
Station Address of this Interface:	The address that Unite CM has on the ESPA bus. Default: 1.
External Station Address:	The address that the remote device has on the ESPA bus. Default: 2.
This Interface is the Control Station:	Select whether Unite CM is the ESPA bus master. Default: Yes.
Extra Carriage Return:	Select whether to add an extra carriage return. Default: No.
Polling During Idle Periods:	Only used if the device is the control station. The remote device has to be polled before it is allowed to send data. Normally polling is done continuously, but some devices cannot handle this. If the remote device cannot handle it, set this option to 'No'. Do not set this parameter to 'No' if the ''Status Mode'' parameter is set to ''Automatic''. Default: Yes.
Status Mode:	Most ESPA devices will reply with status messages automatically. If the remote device does not automatically send status messages, this parameter should be set to ''Request''. Do not set this parameter to ''Automatic'' if ''Polling During Idle Periods'' is set to ''No''. Default: Automatic.
Delay Period for Retry: (0 - 10 000 ms)	If the remote device cannot accept a message, there is a delay period before retrying to transmit the message. Default: 1 000 ms.
Max. Number of Active Pagings:	Sets the maximum number of pagings that will be put in the queue of the remote device. Some devices may not be able to handle too many pagings simultaneously which might result in lost status responses. Default: 1.

ESPA Message Creation

The parameters that can be set in the ESPA Message Creation Settings page are:

Settings	Description
Number of digits in Call Address:	The number of digits that a pager call number has in the ESPA system. Default: 3.
Usage of Number of Digits:	Select what to do when the destination address of a message does not comply with the ''Number of digits in Call Address'' parameter. Default: ''Log warning''.
Number of Transmissions:	The number of transmissions is a value that is transferred to the remote ESPA device. It indicates how many times the remote device will transmit the message to its destination. Default: 2.

Test Source for Message:	Normally the Unite paging subject will be used to create the text for the ESPA paging. In some cases, it might be desirable to use the body of the message or a combination of both. In that case, the body has to contain proper information. Default: ''Unite Paging Subject''.
Subject/Body Separation:	When ''Unite Paging Subject+Body'' is selected for the message text source, this option selects how to separate the subject and body. Default: ''CR + LF''.

Miscellaneous

The parameters that can be set in the ESPA Miscellaneous Settings page are:

Settings	Description
Use Call Status Info Time-out:	If this parameter is set to 'Yes', the status of a call is assumed to be 'paged' after a specified time-out. Default: ''Yes''.
Call Status Info Time-out: (0 - 1 000 s)	If the 'Use Call Status Info Time-out' parameter is set to 'Yes', this parameter specifies the timeout before assuming that the status of a call is 'paged'. Default: 30 s.

Character Code Conversion

The parameters that can be set in the ESPA Character Coding page are:

Settings	Description
Characters 0..255:	These fields specify the value of the byte that will be transmitted on the ESPA bus for ISO8859-1 characters. Accepted values are 0-255 with the exception of ESPA control characters. Please note that values above 127 do not comply with the ESPA standard and may cause problems with some ESPA devices.

10.1.2 TAP Protocol Out

The following settings can be selected or changed in the TAP Out page:

Settings	Description
Enabled:	The TAP configuration can be enabled or disabled. If disabled, the serial port is free to use for other purposes. Default: No.
Name:	Enter a name for the channel.
Serial port:	Port selection (None,1,2): Default: None.
Bitrate:	Select bitrate. Default: 9600 bits/s.
Mode:	Communication mode to use. Default: 8 Data bits, Even parity.
Flow control:	Decides whether flow control shall be used. Default: ''None''.
ASCII conversion table:	This table makes it possible to set up a transformation of display message characters.

11 ASCII Interface

Requires an additional license.

Unte CM has an Ascii interface which makes it possible to interpret alarm and messages from different systems, receive messages via serial ports and enable access to external servers over HTTP. The received data can then be sent to a Unite destination, default the Event Handler in Unite CM.

Received data can also be monitored in Unite CM, see 11.2 Data Monitor on page 112.

11.1 Syntax for ASCII Code Translation

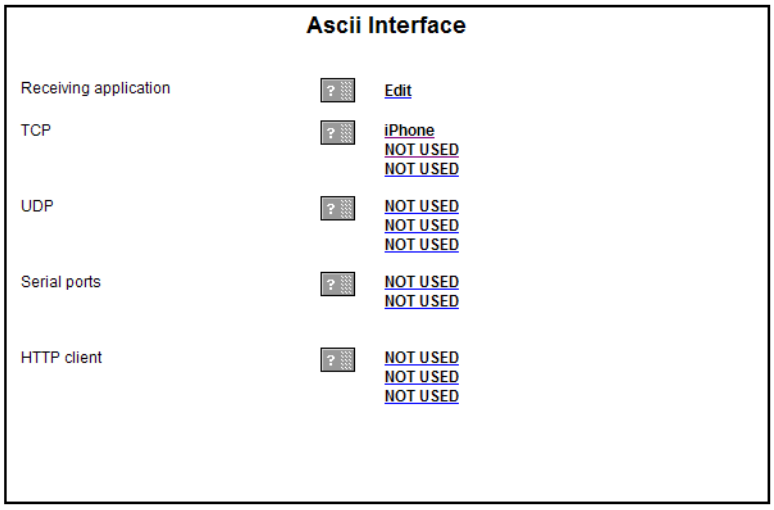
To enter control characters, the Start/Stop string in the TCP Server parameter can be used. The Serial Communication parameter is entered with Ascii code - syntax. A decimal number is written between a backslash and a semicolon, which will then be translated into its character. For example syntax: \4; (= EOT), \6; (=ACK), \28; (= FS), etc.

An ASCII-table for numbers and characters is found in the, Appendix C: ASCII-table on page 37.

1 Click ''Configuration'' on the start page.

2 Select Other > Advanced Configuration in the left menu in the *Configuration* page.

3 Click ''ASCII'' in the menu on the *Advanced Configuration* page.



4 Click ''Edit'' and specify application to receive data.

5 Enter ''IP address/Service'' in the *Destination Address* text field and click ''Activate''.

6 Configure the channel(s)/connection(s) you want to receive data from external systems. See below.

11.1.1 TCP

1 Click a ''NOT USED'' link and configure following TCP parameters:

Setting	Description
Name:	Enter a name for this port
TCP Port:	Enter port to receive data on
Input Start/Stop character string:	Is entered with a syntax code, see 11.1 Syntax for ASCII Code Translation on page 109.
Output Start/Stop character string:	Is entered with a syntax code, see 11.1 Syntax for ASCII Code Translation on page 109.
End of Session as delimiter:	Disabled as default
Restart data capture on receiving Start Word:	Decides if the data capture shall restart when a start character/word is encountered.
Maximum Clients:	Amount of clients that can be connected at the same time.
Close connections initiated by this module:	Decides if the connection shall be closed or stay open until the server shuts down, after data has been sent. Set to ''No'' if a reply is expected.
Responses to unknown connection:	Decides what to do when replying to no longer existing connections. ''Create new'' will use the supplied IP address and port. ''Use existing'' will use an existing connection to that IP address and port. If no such connection exists a new connection will be created.
Character encoding of external data:	Defines how external data shall be interpreted.
Internal data format:	Defines how data is formatted when sent to Unite.
Message to Unite when new connection is established:	The message defined here is sent before any data is received on the new connection.
Message to Unite when connection is disconnected:	The message defined here is sent after all other data has been sent.
Message from Unite to disconnect connection:	When the message defined here is received it will close the connection.

2 Click ''Activate''.

11.1.2 UDP

1 Click a ''NOT USED'' link and configure following UDP parameters:

Settings	Description
Name:	Enter a name for this port
UDP Port:	Enter port to receive data on
Character encoding of external data:	Defines how external data shall be interpreted.
Internal data format:	Defines how data is formatted when sent to Unite.
Remote IP address: (1-5)	Specify IP address(es) to accept data from. If left empty all addresses will be accepted.

2 Click ''Activate''.

11.1.3 Serial ports

1 Click a ''NOT USED'' link and configure following Serial port parameters

Settings	Description
Name:	Enter a name for this port
Serial port:	Select port
Input Start/Stop character string:	Is entered with a syntax code, see 11.1 Syntax for ASCII Code Translation on page 109.
Input Start/Stop character string:	Is entered with a syntax code, see 11.1 Syntax for ASCII Code Translation on page 109.
Baud rate:	Select baud rate used by the connected module
Data Bits:	Select data bits used by the connected module
Stop Bits:	Select number of stop bits used by the connected module
Parity:	Select parity used by the connected module
RTS:	Select how to handle the RTS signal
Restart data capture on receiving Start Word:	Defines if the data capture shall restart when a start character/word is encountered.
Character encoding of external data:	Defines how external data shall be interpreted.
Internal data format:	Defines how data is formatted when sent to Unite.

2 Click ''Activate''.

11.1.4 HTTP client

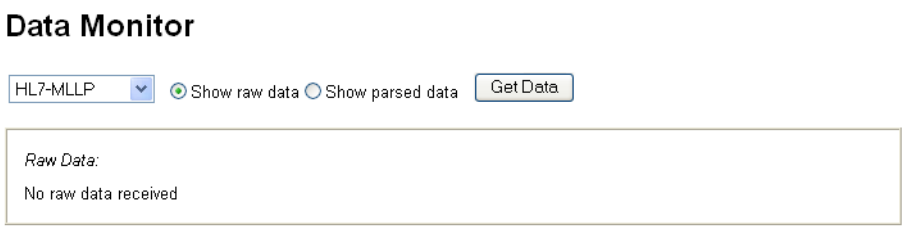
1 Click ''NOT USED'' link and configure following HTTP client parameters

HTTP Client settings	Description
Click on an HTTP client connection to set the parameters, always use the first in the list. The following parameters can be set up:	
Name:	Descriptive name for the HTTP server. Only used in the GUI.
User name:	Defines the name for authentication. Should correspond to the user name for the HTTP server.
User password:	Defines the password for authentication. Should correspond to the password for the HTTP server.
Request timeout:	The time set here must correspond to the time set in other Unite modules and the HTTP timeout in Event Handler.
Additional http header:	Header that will be added when connecting to the HTTP server.

2 Click ''Activate''.

11.2 Data Monitor

This is used to monitor data received by the ASCII input.



1 Click ''Configuration'' on the start page.

2 Select Other > Data Monitor in the menu on the *Configuration* page.

3 Select Input in the drop-down list.

4 Select ''Show raw data'' or ''Show parsed data''.

5 Click ''Get Data''. Information of received data will be shown in the field below.

It is possible make a TCP connection to port 10129 on Unite CM. In real-time you can get the same data that has been presented on this page by sending some commands on the TCP connection.

Commands to use:

- type [raw | message | all]
  type - what type of data to get.
  raw - will look on what is coming in to the module.
  message - will look at the content of the message.
  all - will look in both raw and message.

- source [realtime | cache]
  realtime - is in the beginning empty but will be filled up as data is received.
  cache - stored data.
- channel [name] - what input to look at.
- start - gets data and shows what next to do if some steps are missing.
- stop - stop get data.
- list - lists the available channels.
- help - shows a list of available commands.
  The way to write is to enter the command, all lines ends with carriage return. Space is used to separate the command from the data.

12 Text Displays

NOTE: License is required, see 1.1 Licenses for Unite CM on page 1.

NOTE: Each Unite CM module can control up to 50 corridor displays. Add another Unite CM module to the system in order to extend the system with 50 more corridor displays.

The text displays feature makes it possible to send messages to external displays, such as corridor displays, LED signs etc. The external displays must support the Adaptive Display EZ-95 protocol when using Adaptive displays or the Elen display protocol when using NICD and teleCARE displays. Up to 30 messages can be cycled in a text display and the messages are sorted and removed, first by comparing priority and second by comparing the age.

The text display device must be added as a user in Unite CM with the number tied to the Text Displays category.

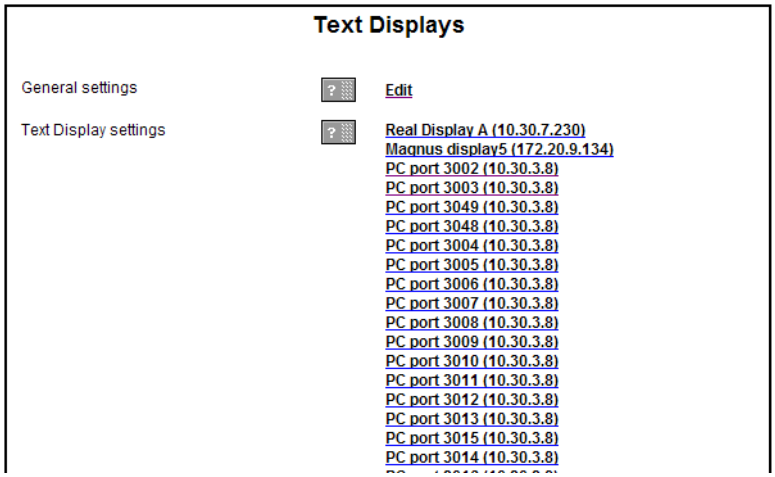
12.1 Text Display Settings

If text displays shall be used, it must be configured as a connected messaging system in the Setup Wizard. Detailed settings are configured from the Advanced Configuration page.

1 Click "Configuration" on the start page.

2 Select Other > Advanced Configuration in the menu on the *Configuration* page.

3 Select "Text Displays" under Output Interfaces, in the menu on the *Advanced Configuration* page. The Text Displays configuration page opens.



4 The parameters that can be set in the Text Displays page are:

Settings	Description
General settings	
Message display time:	Default time for the message to be displayed if there is a new message in the message queue. Can be overridden by a display time set for an individual text display.
Number of stored messages:	Number of messages that can be stored and cycled on each display.
Default TTL:	Default time for the message to be stored if not specified in the message.

Default display type:	The display type selected here will be used as default display type when adding text displays. This can be overridden individually for each display.
Empty message:	Specifies what will be displayed if no messages are stored. How to set the current time (12 or 24 hour clock) as empty message is described in the helptext.
Message refresh time (seconds): NOTE: Only applicable for Adaptive/NICD displays.	Forces the display to refresh even if the message has not changed. Default: ''70'' (disabled by ''0'')
Priority x colour: (x = priority 1 to 9)	The message priority can be visible in the text display with different colors (Red, Green, Yellow). Default: ''Red'' for priority 1-3, ''Yellow'' for priority 4-6 and ''Green'' for priority 7-9
Buzzer off period: NOTE: Only applicable for teleCARE displays.	Specifies the times of the day when a display's buzzer will be muted. The *Buzzer off period* consists of a start time and an end time written in the following format: *hh:mm-hh:mm* (no spaces are allowed in the text string). Example: 00:00-00:00; the buzzer is always muted. Empty field (default); the buzzer is never muted. NOTE: Do not enter overlapping time periods. These settings are valid for all the defined displays, but can be overridden individually for each display.
Text Display settings	
ID:	The identity set here is used as the call number when messages are sent to this text display (max 30 characters).
IP address:	The display's IP address.
IP port:	The IP port used for communication with the text display. Default: ''3001'' NOTE: Default port used by teleCARE display is "2301".
Text display type:	Defines the display type of the connected display. Default: use display type as set under general settings Adaptive: for use with Adaptive display. NICD: for use with Elen display teleCARE: for use with Elen display (teleCARE)

Display width (characters):	Defines number of characters (1 - 100) to be shown in the text display. Longer messages will be truncated. Default: ''16''
Message display time:	Time for a message to be displayed if there is a new message in the message queue. If a time is specified here it overrides the Message display time specified in general settings. Choose default if the general setting shall be used. Default: ''Default''
Buzzer options: NOTE: Only applicable for teleCARE displays.	Defines how the buzzer operates during display of messages. Off - Buzzer is switched off (Default) New calls only - Buzzer sounds when new call is displayed. Every time - Buzzer sounds for every displayed message. Every 5th time - Buzzer sounds for every 5th displayed message.
Display mode: NOTE: Only applicable for teleCARE displays.	Defines how messages is displayed. Scrolling display - The message is scrolled onto the display from the bottom. NOTE: When there is only 1 active message the display will not scroll. Constant display - The message is shown directly. At the end of the display time the display is blanked for 300 ms before the next message is shown. Default: Scrolling.
Buzzer off period: NOTE: Only applicable for teleCARE displays.	Specifies the times of the day when a display's buzzer will be muted. The *Buzzer off period* consists of a start time and an end time written in the following format: *hh:mm-hh:mm* (no spaces are allowed in the text string). Example: 00:00-00:00; the buzzer is always muted. Empty field (default); the buzzer is never muted. NOTE: Do not enter overlapping time periods. If the field(s) is empty, the corresponding settings located under *General setting* will used.

5 Click ''Activate''.

13 SMS via GSM Modem

NOTE: Requires an additional license

IMPORTANT: The GSM interface on the Unite CM consists of a java application. This means that it is not possible to upload and run an additional java application on the Unite CM if the GSM interface is used.

It is possible to send SMS from Unite CM to GSM phones and to send SMS between GSM phones and handsets in the system. This option is very useful for diversion purposes.

A GSM modem is required and the GSM phone must be added as a user in Unite CM with the number tied to the GSM category.

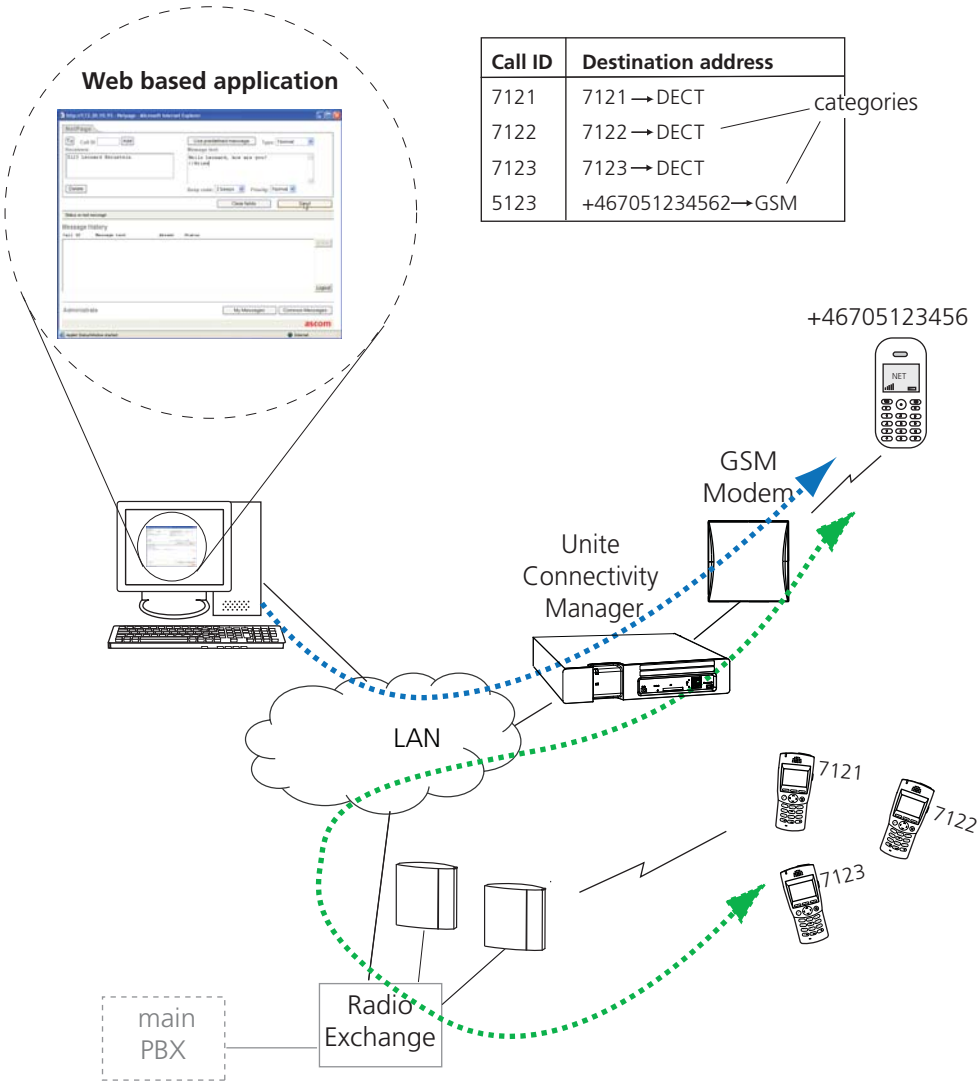


Figure 52. SMS via GSM modem.

13.1 Add GSM User

NOTE: If you use a SIM with a PIN code, either remove the code before placing the SIM in the GSM modem or change the pinCode.txt on the FTP area on Unite CM.

1 Log on to Unite CM with an FTP client. Note that how to log on can differ between different FTP clients.[1]

Default username is ''ftpuser'' and default password is ''changemetoo''. xxx.xxx.xxx.xxx is the host name.

Examples:

- Windows Explorer: fill in ''ftp://username:password@xxx.xxx.xxx.xxx'' in the address field.
- Firefox: fill in ''ftp://xxx.xxx.xxx.xxx'' in the address field and log on with ''username'' and ''password''.

2 Download the following files located in the *client* folder:

- pinCode.txt
- Parameters.txt

3 Enter your PIN code in *pinCode.txt*

4 Set the baud rate used by Unite CM by editing *Parameters.txt*

5 Upload the changed files.

6 Restart the module.

Now we assume the following:

- the GSM modem is connected to serial port 1 (COM1) on Unite CM.
- Unite CM has license for GSM modem interface and the GSM check box is selected as Connected Messaging System in the setup wizard during the setup.

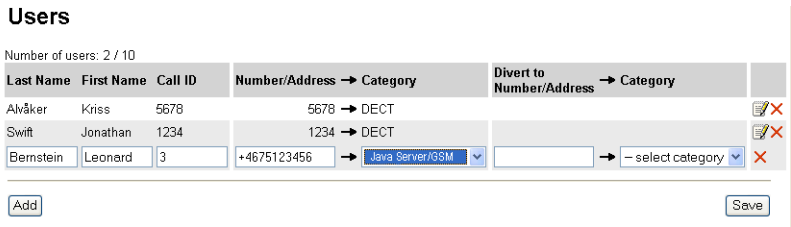
1 Click ''Users & Groups'' on the start page.

2 Select Messaging > Users and click ''Add''.

3 Enter the name and a Call ID. The Call ID can be any number or a text.

4 Enter the GSM phone number in the Number/Address text field.

5 Select ''Java Server/GSM'' in the Category drop-down list.



6 Click ''Save''.

13.2 Send Message from Unite CM to GSM User

Sending a message to the GSM phone (with the possibility to accept or reject the message) is done the same way as to handsets in the system, see 19.1 Create and Send Messages via the Messaging Tool on page 147 or 19.2 Create and Send Messages via NetPage on page 148.

1.Internet Explorer is not an FTP client so its not possible to copy and move files from Internet Explorer.

13.3 Send SMS from GSM Phone to a Handset in the System

The SMS must have a hash ''#'' in front of the handset No. and a space between the No. and the message, for example: #7121 Hi Kriss, how are you, where 7121 is the handset number.

14 SMTP Mail Interface

NOTE: Requires an additional license.

Unite CM can receive e-mails from any application capable of sending SMTP e-mails, and forward them as messages to handsets in the system. Acknowledgement and delivery reports can also be sent back to origin sender.

Requirements

- User dependant filters and redirect of e-mails must be set up in the user's mail client, if e-mail notification is wanted.
- The company mail server must be set up to allow sending e-mails to Unite CM. This includes relaying and possibly firewall configuration (Contact your local IT department).
- The company mail server must be set up to allow relaying to be able to send messages from the Ascom Messaging System to e-mails. (Contact your local IT department).

14.1 Considerations for Local IT Department

Depending on the application, the local IT department must be involved regarding settings for the mail server, e-mail client, Unite CM, firewall and DNS (domain name server).

Receiving e-mails from Corporate Mail Server

- The mail server must know that Unite CM exists and be able to send e-mails to Unite CM. Relaying to Unite CM must be allowed and the IP address must be known.
- If the firewall is situated between the mail server and Unite CM, it must be configured to enable SMTP between the mail server and Unite CM.
- An mx-record for the Unite CM host has to be set up in the DNS like unitecm.company.com
- The E-mail client must set up the rule ''redirect'' of e-mails for E-mail notification.

Sending e-mails directly to Unite CM

- The local IT Department should only be required to supply the IP address and the host name of Unite CM and, if needed, enabling communication through the firewall.

Transfer a reply from a handset as e-mail / Create an e-mail based on an Event

- The mail server must allow sending e-mails from Unite CM. This requires relaying from Unite CM.
- If the firewall is situated between the mail server and Unite CM, it must be configured to enable SMTP between the mail server and Unite CM through the firewall.

14.2 Mail Addressing Options

It is possible to set certain properties for the message by adding a pseudo protocol in the destination mail address. The following properties can be set:

- Beep code
- Message priority
- Request for manual acknowledge (positive and negative)
- Request for user response data

The format for the protocol is:
<call number>.b<beep code>.p<priority>.a<answer type>

The call number is the identity of the handset, for example 9420. The beep code, priority and answer type can be set as described below:.

Beep code (.b)	Priority (.p)	Answer type (.a)
0 (silent)	-	0 (no answer=default)
1 (default)	1 (highest)[1]	1 (manual acknowledge)[2]
2	2	2 (user response data)[3]
3	3	
4	4	
5	5	
6	6	
7(siren)	7 (default)	
	8	
	9 (lowest)	

[1] Priority 1 must be restricted to handle very high alerts like fire alarm or cardiac alarm. Frequent use of this priority level might have severe impact on your Messaging system.

[2] The user will have the alternative to either accept or reject the message from the handset. The subject of the returned e-mail is set to ''User acknowledge'' and the body contains the string ''Accepted'' or ''Rejected'', according to parameter text entered, see 14.2.2 SMTP Output Interface (send reply message as e-mail) on page 123.

[3] The user response data option will result in an interactive message (not supported by all equipment) with the possibility to reply to the original sender. When selected, the user can input arbitrary text as a reply. The subject of the returned e-mail is set to ''User response'', according to the parameter text entered, see 14.2.2 SMTP Output Interface (send reply message as e-mail) on page 123. The body will contain the entered data.

Examples of the Mail address Option:

Example 1:

9746.b2.p3.a1@unitecm.company.com

This will result in a message to the call number 9746, with beep code 2, priority 3 and a request for manual acknowledge.

If any properties are left out default values will be used.

Example 2:

9746.a2@unitecm.company.com

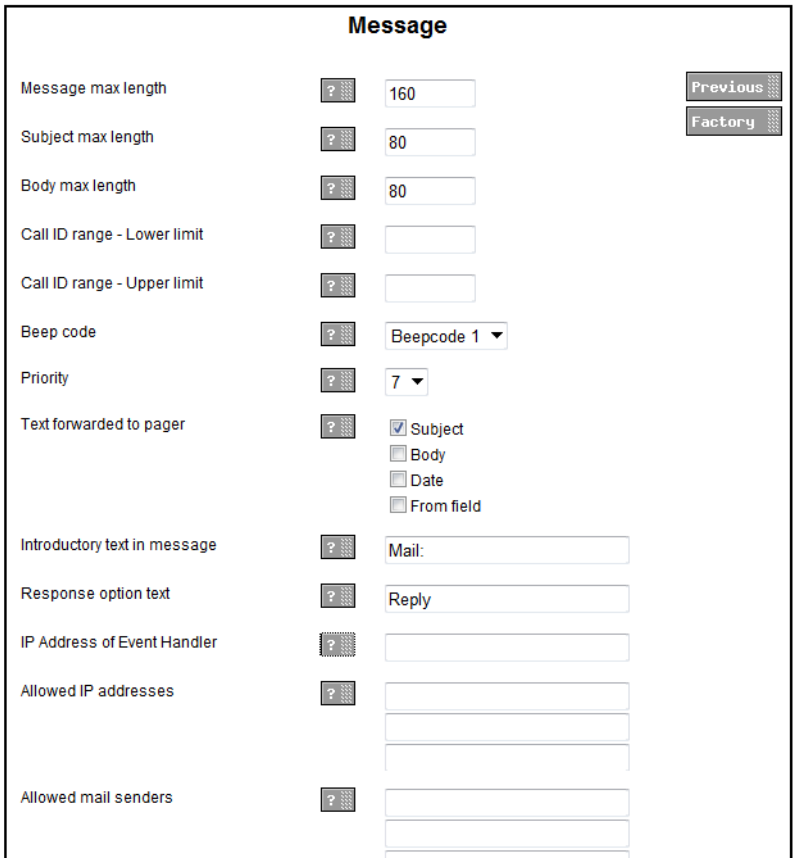
This means that the receiver alias number is 9746, beep code is by default set to 1 and the priority is by default set to 7. User response data is requested.

14.2.1 SMTP Input Interface (receive e-mail as message)

1 Click ''Configuration'' on the start page.

2 Select Other > Advanced Configuration in the menu on the *Configuration* page.

3 Click "SMTP" under Input Interfaces, in the menu on the *Advanced Configuration* page.



4 The following settings can be selected/changed:

Settings	Description
Message max length:	Max. numbers of characters to be forwarded to the handset. Overflow is truncated.
Subject max length:	Max. numbers of subject characters to be forwarded to the handset.
Body max length:	Max. numbers of body characters to be forwarded to the handset.
Call ID range - Lower limit:	Lower limit for the allowed Call ID range. If a message is sent to a Call ID out of the range, the message will be discarded.
Call ID range - Upper limit:	Upper limit for the allowed Call ID range. If a message is sent to a Call ID out of the range, the message will be discarded.
Beep code:	Characteristic of the beep.
Priority:	The message priority. A low number means high priority. 7 = normal paging.
Text forwarded to pager:	What part(s) of the e-mail that shall be forwarded to the handset can be specified.
Introductory text in message:	Text in front of the forwarded e-mail (note: the characters are included in max. message length)
Response option text:	Text in messages with response option.

IP Address of Event Handler	The IP address of the Unite module with Event Handler. The Event Handler determines which action to be done when receiving the message. When this parameter is set, all incoming messages will be sent to the Event Handler instead of sending the message to its origin destination. Additional settings are required in the Event Handler. See also 4.11 Advanced Event Handling on page 51.
Allowed IP addresses:	If e-mail shall be accepted from specific mail servers / clients only, the IP addresses must be specified here.
Allowed mail senders:	If e-mail shall be accepted from specific sender addresses only, the e-mail addresses must be specified here.

5 Click ''Activate''.

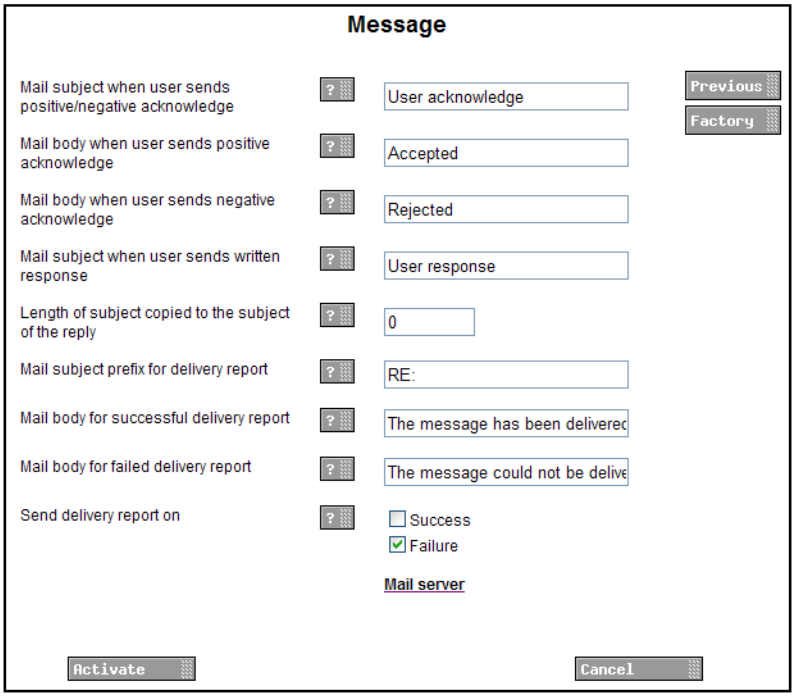
14.2.2 SMTP Output Interface (send reply message as e-mail)

Subject text and body text in acknowledgement and delivery reports back to origin sender can be modified.

1 Click ''Configuration'' on the start page.

2 Select Other > Advanced Configuration in the menu on the *Configuration* page.

3 Click ''SMTP'' under Output Interfaces, in the menu on the *Advanced Configuration* page.



4 The following settings can be selected/changed:

Settings	Description
Mail subject when user sends positive/negative acknowledgement:	Subject text in acknowledgement sent to origin sender.

Mail body when user sends positive acknowledge:	Body text in positive acknowledgement sent to origin sender.
Mail body when user sends negative acknowledge:	Body text in negative acknowledgement sent to origin sender.
Mail subject when user sends written response:	Subject text in interactive message reply sent to origin sender.
Length of subject copied to the subject of reply:	Number of characters copied from subject into the reply subject.
Mail subject prefix for delivery report:	Prefix text for delivery reports back to origin sender.
Mail body for successful delivery report:	Text sent back to origin sender when message delivery was successful.
Mail body for failed delivery report:	Text sent back to origin sender if message delivery failed.
Send delivery report on:	Specifies when a delivery report shall be sent.

5 Click ''Activate''.

NOTE: If the IP address to the company Mail Server has not been defined it must be set now. A link to the ''Mail Server'' setting is found on the Message page. The mail server address can also be set in the wizard or from the Advanced Configuration page.

15 DECT Interface

It is recommended to configure the carrier system interfaces from the Wizard, but it can also be done from the Advanced Configuration page.

This chapter describes configuration from the Advanced Configuration page, for some carrier systems. It does not include all supported carrier systems.

The Unite CM can be connected to one carrier system (see 15.1 DECT Phone System) or to several carrier systems simultaneously, see 15.2 Mixed DECT Systems.

15.1 DECT Phone System

15.1.1 Alcatel OmniPCX Enterprise

Communication with the Alcatel OmniPCX Enterprise is done over the LAN. To be able to receive alarms and user data from handsets in the system, a CMP board has to be installed in the OmniPCX Enterprise. For configuration of the Alcatel OmniPCX Enterprise and installation and configuration of the CMP board, see separate documentation from the vendor.

15.1.2 Ericsson BusinessPhone, DCT1800-GAP, DCT1800-S and DCT1900

For configuration of the DECT Phone System, see separate documentation from the vendor.

1 Connect the delivered cable to the serial port 1 (COM1) port on Unite CM.

2 Connect the cable to the I/O port on the IC-CU2 board on the DECT Phone System.

See Appendix B, for a description of the cable.

15.1.3 MX-ONE/MD110, Enterprise Mobility Node, Ascotel IntelliGate, MD Evoluition

Communication with the DECT Phone System is done over the LAN. For configuration of the DECT Phone System, see separate documentation from the vendor.

15.1.4 IP-DECT

Figure 53. Redundancy achieved by connecting Unite CM to two IP-DECT base stations and setting primary and secondary IP addresses.

Unite CM can communicate with the IP-DECT system over a LAN.

It is possible to set an address to a secondary IP-DECT master which is used as a redundancy backup. The secondary IP Address is used if the connection to the primary IP Address is lost. If the secondary IP Address is lost, Unite CM will try to use the primary IP Address.

To do IP-DECT IP address settings, do as follows:

1 Click ''Configuration'' on the start page.

2 Select Other > Advanced Configuration in the menu on the *Configuration* page.

3 Restart Unite CM (not needed if configured from the Wizard).

4 Select ''IP-DECT'' in the menu on the *Advanced Configuration* page.

5 Continue in A) IP-DECT system with a Single Master or B) IP-DECT system with Multiple Masters below.

A) IP-DECT system with a Single Master

1 Enter the IP address to the DECT system

2 Enter a secondary IP address if two DECT system are used for redundancy purposes, enter the IP address to the secondary DECT system in the *Secondary DECT IP Address* text field.

B) IP-DECT system with Multiple Masters

Multiple DECT interfaces are used for connections to an IP-DECT multi-master system with a common PBX number plan.

NOTE: All numbers in the system must be unique, i.e. a number for a user in one system cannot be the same as a number for a user in another system.

1 If not already set via the wizard, click the *Multiple Locations* link, select ''Yes'' and reboot the module.

2 Select IP-DECT in the menu and click a ''NOT USED'' link.

3 Enter a name for the DECT interface.

4 Enter the Master IP address.

5 Enter the Standby Master IP address if a secondary Master is used as a backup.

6 Configure desired number of interfaces. Up to 20 DECT interfaces can be set up. The relative order when entering the IP-DECT Masters makes no difference.

7 If data shall be encrypted for multiple IP-DECT locations, click the *Encrypt data* link and select ''Yes''.

Every configured connection is supervised every 60 seconds. If the supervision fails the connection is handled as lost and a persistent fault is generated. After solving a problem with a lost connection, it can take up to one minute before the connection over the DECT interface is restored. During that time the connection is considered lost and no messages will be sent to that specific connection.

15.2 Mixed DECT Systems

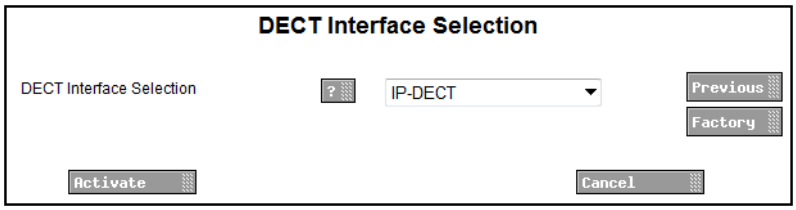
It is possible to connect different kinds of DECT systems to a Unite CM. The systems that can be connected are MX-ONE/MD110 and IP-DECT. This feature is useful when you want to connect only one Unite CM to different DECT systems.

NOTE: Configuration of mixed DECT systems cannot be done via the Wizard. The MX-ONE/MD110 must be configured to use port 1817 when communicating with a Unite CM configured with a mixed DECT system that uses encryption.

1 Click ''Configuration'' on the start page.

2 Select Other > Advanced Configuration in the menu on the *Configuration* page.

3 Select "Interface Selection" under *DECT Interface* on the *Advanced Configuration* page.

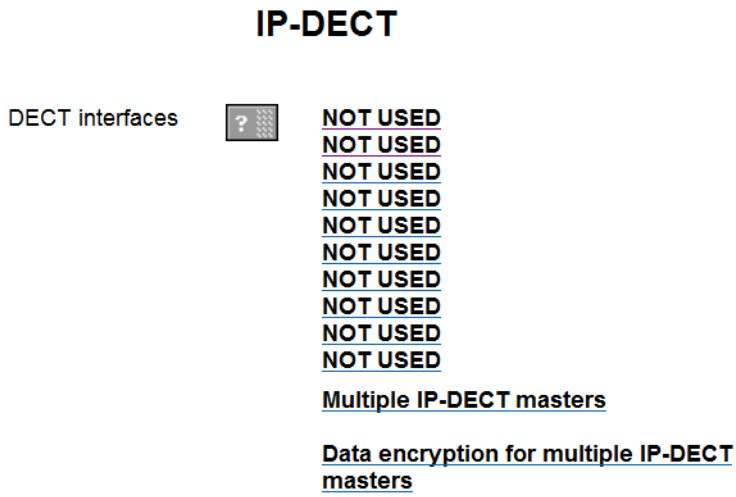


4 In the *DECT Interface Selection* drop-down list, select "IP-DECT"

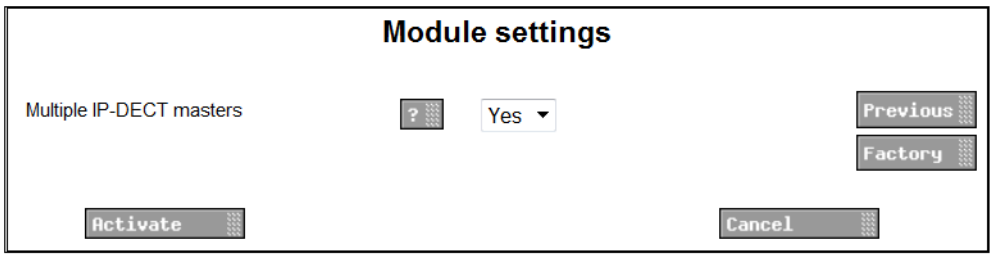
5 Click "Activate".

6 The Unite CM must reboot to apply the setting. Click the link "Click here to reboot" and then click "Reboot".

7 When the Unite CM has been rebooted, select "IP-DECT" under *DECT Interface* on the *Advanced Configuration* page.



8 Click "Multiple IP-DECT masters".



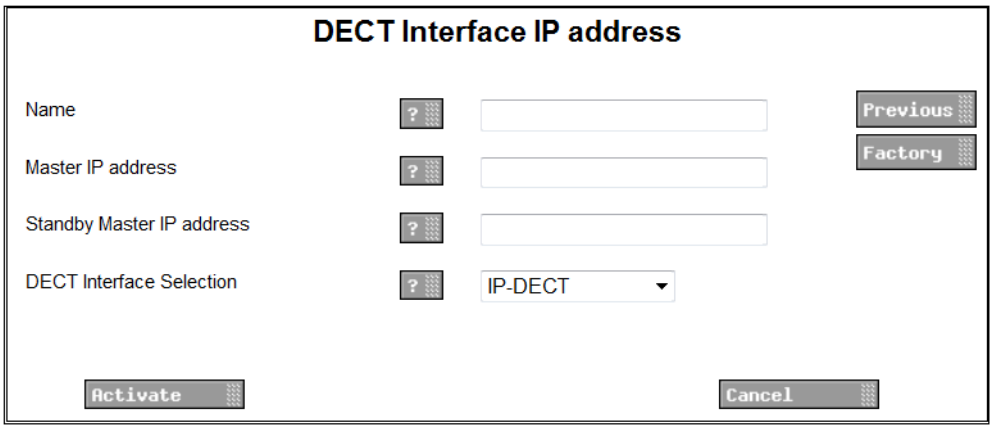
9 In the *Multiple IP-DECT masters* drop-down list, select "Yes".

10 Click "Activate".

11 The Unite CM must reboot to apply the setting. Click the link "Click here to reboot" and then click "Reboot".

12 When the Unite CM has been rebooted, select "IP-DECT" under *DECT Interface* on the *Advanced Configuration* page.

13 Configure the DECT interface to be connected to the Unite CM by clicking on a "NOT USED" link.



14 Enter the following:

Name:	Description to identify the DECT interface. The description will appear in the DECT interface list
Master IP address:	The IP address to primary DECT system. That is, the IP-address of IP-DECT Master or IP-address of MX-ONE/MD110.
Standby IP-address:	The IP-address to the secondary DECT system used as backup if the primary DECT system goes down. (Optional)
DECT Interface Selection:	The type of DECT interface to be used.

15 Click "Activate"

16 Repeat steps 13 - 14 to add additional DECT systems.

15.3 DECT Interface settings

The DECT Interface controls the messaging flow between the Cordless Telephone System and other system modules, for example UNITE compliant modules and System 900 modules.

15.3.1 General Settings

To find DECT General Settings, do as follows:

1 Click ''Configuration'' on the start page.

2 Select Other > Advanced Configuration in the menu on the *Configuration* page.

3 Click ''General Settings'' in the menu on the *Advanced Configuration* page.

- Call Diversion Display Text
  When this parameter is enabled, the text specified is added to the display message when a call diversion takes place. The original Call ID can be included in the parameter text by writing a % character where the Call ID shall be inserted.

Advanced parameters include:

- Extended Activity Log
  In addition to when a Unite block is delivered to a handset, activity log information is also sent to the Log Viewer when the block is received by the DECT interface. The extra information can only be displayed in Log Viewers that are updated continuously and if activity logs are configured in Unite CM. This function should be used with care as it generates heavier network load. For more information about extended activity logs, see Function Description, Activity Logging in Unite, TD 92341GB.
- Set time in DECT?
  It is possible to set the time in DECT when the parameter is set to ''Yes''. It is only possible when DCT1800-GAP systems with CPU2 software is used. If the parameter is set to ''Yes'', Unite CM sets the time in DECT on startup and on each day at the time set by the Time push time parameter.
- Priority Conversion
  Used to convert messaging priorities; Alarm, High, Normal and Low. This conversion is normally only used for compatibility with some PWT handsets and should never be enabled unless you are absolutely sure.
- IM update status handling
- No of included 9dLD locations
  Only valid in combination with Ascom messaging system.

15.3.2 System Dependent Settings

Which parameters that can be changed is dependent on the DECT Phone System that Unite CM is connected to.

BusinessPhone, DCT1800-GAP, DCT1800-S, DCT1900, MD Evolution and Enterprise Mobility Node

There are no system dependent features for these systems.

MX-ONE/MD110, Ascotel IntelliGate, and OmniPCX Enterprise

- IP address

  Since the MX-ONE/MD110, Ascotel IntelliGate and MD Evolution is connected over the LAN, the IP address of the MX-ONE/MD110, Ascotel IntelliGate or MD Evolution has to be entered.
- Port Numbers
  - Unite CM always uses port 1814 for communication with the MX-ONE/MD110. This port has to be defined in the MX-ONE/MD110 as well. The MX-ONE/MD110 must be configured to use port 1815 when communicating with Unite CM. The MX-ONE/MD110 must be configured to use port 1817 when communicating with a Unite CM configured with a mixed DECT system that uses encryption.
  - The default port for communication with Ascotel IntelliGate is 2775.

NOTE: If Unite CM replaces a 9dMMS, check that other port numbers than the ones above are not used for the communication between the 9dMMS and the MX-ONE/MD110.

IP-DECT

- DECT IP address

  Since the IP-DECT Master is connected over the LAN, the IP address of the IP-DECT Master has to be entered.
- Secondary DECT IP address

  If two DECT systems are used for redundancy purposes, the IP address of the secondary DECT system needs to be entered.

15.3.3 DECT Message Distribution

The DECT Interface has distribution lists that define where incoming data from handsets, for example alarms and user data, should be sent.

To find settings for DECT Message Distribution, do as follows:

1 Click ''Configuration'' on the start page.

2 Select Other > Advanced Configuration in the menu on the *Configuration* page.

3 Click ''Messaging Distribution'' under DECT Interface in the menu on the *Advanced Configuration* page.

The following information is supported:

- Alarm
  - Personal alarms with location information from handsets in the Cordless Telephone System.
- Mobile Data
  - User data sent from handsets in the Cordless Telephone System.
- Location
  - Special Location[1] information from handsets in the Cordless Telephone System. This information can be used to track the route of a handset in a building.
- Availability
  - Includes absence information, i.e. if a handset is placed in Charging/Storage Rack.

The addressing of the receivers is described in Installation Guide, Elise3, TD 92679GB.

1.The Special Location can be sent every time a cordless handset gets a new location code from a location device in the system. This requires configuration both in the handset and in the location device. Also called ''Immediate Alarm Transmission''.

15.3.4 SMS Character Set

This setting determines which characters that can be displayed in the handsets when they receive messages. Additionally, the setting also determines which characters that can be entered in the handsets when the users write messages.

NOTE: The number of characters that can be entered in the handset when writing a message depends on which SMS character set that is used.

1 Click ''Configuration'' on the Start page.

2 Select Other Settings > Advanced Configuration.

3 Select ''SMS Character Set'' under *DECT Interface* in the menu on the *Advanced Configuration* page.

4 Select one of the following:

- Standard SMS (Compatibility Mode)	Standard SMS works with all handsets but some special characters may not be correct.
- Latin-1	Used for later generation of handsets.
- UTF-8	Used for later generation of handsets. Use UTF-8 to include characters that is not included in the Latin-1 character set. NOTE: The UTF-8 character set requires an Ascom IP-DECT system with version 5.1.2 or later.

5 Click ''Activate''.

15.4 Absence Handling in DECT

Unite CM keeps track of handsets that have reported absence status. When a message is sent to an absent handset, the sending module can get information from Unite CM that the handset is absent.

There are several ways to report that a handset is absent to the Unite CM:

- The user of the handset sets the handset to absent via the handset's GUI (Manual absence). The status of the handset will be shown in the Absence List. See 15.4.1 Absence List on page 132.
- The user of the handset put the handset in a charger. The handset must in this case be configured to change to absence when it is put in charger (Rack absence). The status of the handset will be shown in the Absence List. See 15.4.1 Absence List on page 132.
- Unite CM can treat a handset as absent when the handset is offline[1], even when manual absence or rack absence are not set in the handset. See 15.4.3 Absence Status for Offline Devices on page 132

NOTE: This feature requires that one and same Unite CM has device management and messaging enabled. See 20 Messaging Administration on page 156 and 6.1 Device Management Setup on page 74.

1."Offline" means that the handset is out of range, turned off, or out of battery.

15.4.1 Absence List

A list in Unite CM indicates which handsets that have reported absence status. The handset only appears in the list when the user of the handset activates Manual absence or Rack absent.

NOTE: A handset that is logged out/turned off will not appear as absent in the list. However, the Unite CM can treat a handset as absent even when it is logged out/turned off. See 15.4.3 Absence Status for Offline Devices on page 132.

1 Click ''Configuration'' on the start page.

2 Select Other > Advanced Configuration in the menu on the *Configuration* page.

3 Select ''View Absence List'' in the left menu in the menu on the *Advanced Configuration* page. The Absence List opens.

The handset identity and absence type are shown:

- Manual absent — The handset has been set in *Message absence* mode by the user of the handset.
- In storage rack (Rack absent) — The handset is put in a charger.

  NOTE: Depending on handset, the *In charger action* might also be set to *Message absence* in the handset.

It is possible to manually remove a handset from the absent list by clicking the corresponding ''Remove'' link. When clicking "Remove", the Unite CM will consider the handset as present.

15.4.2 Clear Absence List

The absence list in Unite CM can be cleared. This has to be done, for example, when a Unite CM is reinstalled in a system since the absence list then will be out of date. This should only be used as a last resort if there is a permanent mismatch in the system.

1 Click ''Configuration'' on the start page.

2 Select Other > Advanced Configuration in the menu on the *Configuration* page.

3 Select ''Clear Absence List'' in the menu on the *Advanced Configuration* page.

4 Click the ''Clear'' button.

NOTE: When the absence list is cleared, Unite CM will consider handsets that currently are placed in a charger or manually set to absent as present.

15.4.3 Absence Status for Offline Devices

When Manual absent or Rack absent is not set in an offline[1] handset, it is possible to let the Unite CM to treat the handset as absent. Use this feature to make sure that the sending module (for example Netpage) will treat an offline handset in the same way as an absent handset that is online.

When this feature is enabled and the handset is offline, it will not appear as absent in the Absence List. The handset will only be indicated as absent in the application (for example Netpage) that sends a message to the handset.

Note that this parameter only will have affect when a handset has no absent set and then goes offline. If a handset with absent set goes offline, the existing absent status will be reported to the Unite CM - even when this feature is enabled.

1."Offline" means that the handset is out of range, turned off, or out of battery.

NOTE: This setting also affects how offline WLAN handsets should be treated.

1 Click ''Configuration'' on the start page.

2 Select Other > Advanced Configuration in the menu on the *Configuration* page.

3 Click "Absence Handling".

4 In the *Treat offline devices as absent* drop-down list, select how offline handsets should be treated.

5 Click "Activate" to save the setting.

15.5 Base Station Conversion

The base station IDs that are received together with personal alarms can be converted to another ID before it is sent to the system.

15.5.1 Background

In some systems, the base station IDs might alter when the Cordless Telephone System is upgraded. In the alarm handling the base station IDs are used for location determination of an alarming handset. Normally the ID is converted to a text string that describes the location. The ID can also be used in trigger conditions, for example to decide which guards that should be informed about an alarm. To avoid having to update the base station IDs in many different places in the configuration of the alarm handling, Unite CM can convert the base station IDs before it is sent to the alarm system.

This can be convenient regardless of how the Cordless Telephone System handles an upgrade as the base station IDs normally consists of about ten characters. The base station conversion can then be used to shorten the IDs before it is sent to the alarm system. It is also possible to convert the ID to a descriptive text.

15.5.2 Configuration

The Base Station Conversion can be reached from the *Advanced Configuration* page.

1 Click ''Configuration'' on the start page.

2 Select Other > Advanced Configuration in the menu on the *Configuration* page.

3 Select ''Base Station Conversion'' under DECT Interface in the menu on the *Advanced Configuration* page.

4 Enter the file name or click ''Browse'' and select the file.

5 Click ''Import file''.

The conversion table is imported as a CSV file, with the base station ID in the first column and the new ID in the second. The new ID is a string of maximum 50 characters. IDs that are not included in the table will be sent to the alarm system without any conversion.

16 Cisco Interface

Cisco interface is a gateway between the Unite messaging system and Cisco IP phones, and sends messages from Unite to Cisco. It contains a simple configuration GUI and interacts with the Cisco Unified Communications Manager (CUCM) and the Cisco IP phones.

The CUCM is the central node in a Cisco phone network with information about all handsets and calls. It also keeps track of which handsets that exist and which handsets that are connected.

The configuration is done both in the Cisco interface and in the CUCM. The Cisco interface contains settings for communications with the phones, communication with the CUCM and translations. In the CUCM users are created and handsets are associated to the users.

16.1 CUCM Configuration

The administration of users and devices is done in the CUCM. Users are added and phones are associated to the users.

1 Go to the home page of the CUCM.

2 Create a new user.

The default *Phone user* used in the Cisco interface is called *UniteSystem*, this can be changed in the configuration of the Cisco interface.

3 Associate the user to all phones that shall be used.

4 Set SNMP parameters.

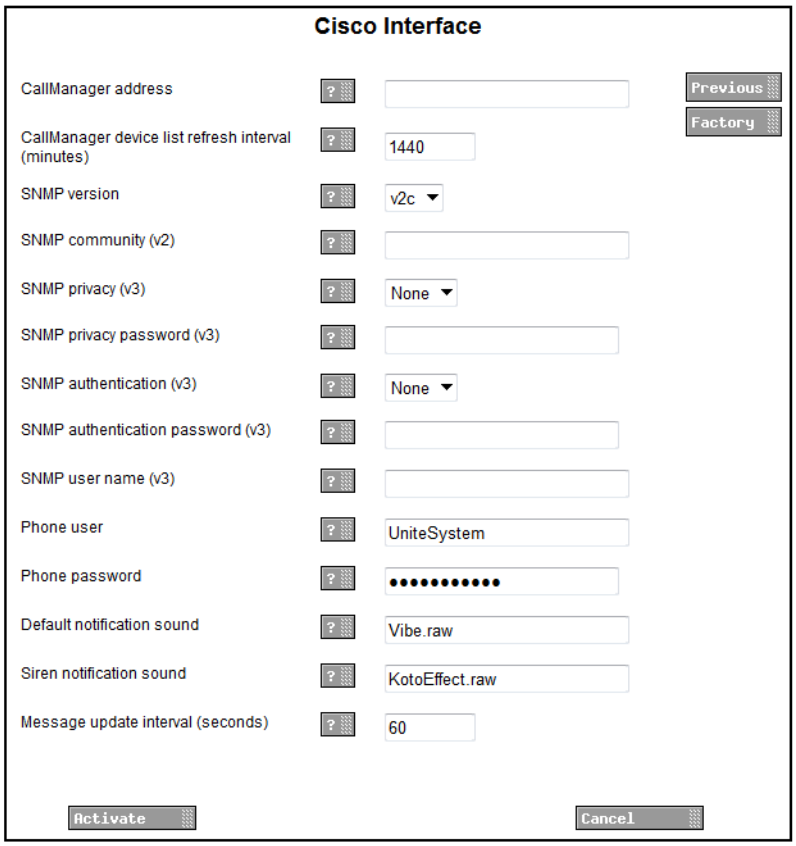
16.2 Cisco Interface Configuration

The ECG uses SNMP to obtain the configured devices in the CUCM. The ECG supports both SNMP version 2 and 3, depending on the customer's requirements.

1 Click ''Configuration'' on the start page.

2 Select Other > Advanced Configuration in the menu on the *Configuration* page.

3 Select ''Settings'' under *Cisco Interface* on the *Advanced Configuration* page.



NOTE: Make sure that the phone user and the handset password is the same as in the setup for the CUCM, and that the SNMP parameters correspond to the SNMP parameters in the CUCM.

4 In the *CallManager address* text field, enter IP address of the CUCM.

5 In the *CallManager device list refresh interval (minutes)* text field, set the refresh interval value.

The complete device information is read at regular intervals, default once a day. To refresh too often in systems with huge amount of devices puts a heavy load for the CUCM. In large systems it is recommended to increase the interval time for reading the list of telephone numbers from the CUCM.

6 In the *SNMP version* drop-down list, select SNMP version to use for the communication with the CUCM.

7 Set the SNMP parameters corresponding to the settings in the CUCM.

The only required parameter for SNMP version 2, is the community name.

- SNMP community, version 2 only

For increased security in SNMP version 3, the following need to be set.

- SNMP privacy (encryption method)
- SNMP privacy password (encryption password)
- SNMP authentication (authentication method)
- SNMP authentication password
- SNMP user name for connecting

8 Use the same phone user and phone password that was given the user in the CUCM. See 16.1 CUCM Configuration on page 134 step 2.

9 Optionally, in the *Default notification sound* text field and *Siren notification sound* text field, change the file name of the default notification sound and the siren sound.

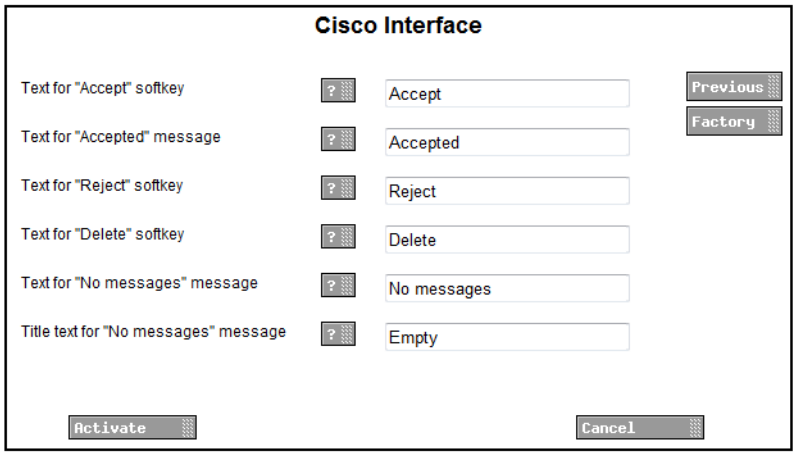
10 Optionally, in the *Message update interval (seconds)* text field, change the message update interval. The default is 60 seconds, which means that a message update will be sent to the handset every 60 seconds until a response of the message is selected by the handset user.

11 Click "Activate".

16.3 Translations

This is where to set the text for soft keys which are displayed on the handset when receiving a message. The soft keys differ from different Unite messaging types. The length of the text can differ depending on the model of handset that is used. The text should be as short as possible.

In the corresponding text field, enter the name of the soft key to be displayed depending on which type of message that is received.



17 WLAN Interface

17.1 Handset Registration

To be able to register to Unite CM, each VoWiFi handset must be programmed with the IP address of Unite CM used, refer to the Configuration Manual for respective VoWiFi handset.

17.2 Shared Phones

When using shared phones all VoWiFi handsets authenticates with passwords. The password can be a common password for all users or the call number. Individual passwords are supported by the User Server in Unite CM.

In order to work, all shared phones in a system need to have the same ''major'' version in the software version.

17.3 WLAN System

WLAN system handles the VoWiFi handset relogin time and authentication. A handset is considered to be logged out if it has not made a relogin within a certain time. Call diversion display text and Extended activity logging is also enabled in this view.

To find settings for WLAN System, do as follows:

1 Click ''Configuration'' on the start page.

2 Select Other > Advanced Configuration in the menu on the *Configuration* page.

3 Click ''WLAN System'' under WLAN Interface, in the menu on the *Advanced Configuration* page.

4 Enter/select the following settings:

- The time before a handset must relogin to Unite CM is set in minutes and when this time is exceeded the handset will be considered unreachable. This is the maximum time it takes for a handset to reconnect after installing a new Unite CM or updating a Unite CM. Note that a short relogin time implies a higher service/security but it also loads the system.
- Text specified in the ''Call Diversion Display Text'' text field is, if enabled, added to the display text when a call diversion takes place. By entering the character ''%'', the original Call ID will be included in the display text on the place where the character is entered. Note that some characters are special characters that are not visible.
- Enable Extended Activity Log for intermediate logs, for more information refer to the Function Description, Activity Logging in Unite TD 92341GB.
- The very first time a VoWiFi handset logs in to Unite CM, it must authenticate itself with a password. The password is then stored in the handset for future authentication. Unite CM has three authentication alternatives; ''Common password'', ''User server'' and ''Number as password''.
- A common password can be specified in Unite CM and this password is then used for all VoWiFi handsets in the system. If the common password field is left empty, the handset must send an empty password for authentication.

  If individual passwords are needed, for example for shared phones, passwords can either be specified in a User Server or the individual call numbers can be used, refer to chapter 4.2 Additional User Settings on page 23.
- Forced login allows a user to login with a call number that already is in use. The handset that already is logged in will then be unregistered.

The function is only valid when the authentication method is set to ''Common password'' or to ''Number as password''.

- External location server
  An external location server can be used for obtaining location information about a device. When enabled, the timeout specifies the maximum time an alarm will wait for location data from the location server, before the alarm is distributed to the alarm recipients, i.e. what delay is acceptable in your specific system.
- External location server address
  Enter the location server address in the format IP address/service. If only IP address is specified, EventHandler will be used as a default service.

5 Click ''Activate''.

17.4 WLAN Message Distribution

The WLAN Interface has distribution lists that define where incoming data from handsets, for example alarms and user data, should be sent.

To find settings for WLAN Message Distribution, do as follows:

1 Click ''Configuration'' on the start page.

2 Select Other > Advanced Configuration in the menu on the *Configuration* page.

3 Click ''Message Distribution'' under WLAN Interface in the menu on the *Advanced Configuration* page.

The following information is supported:

- Alarm

- Personal alarm from VoWiFi handsets.

• Mobile Data
- User data sent from VoWiFi handsets.

• Availability Info
- Change of status of the VoWiFi handsets.
(The status can be changed from Unite CM GUI or from the VoWiFi handset).

The addressing of the receivers is described in Installation Guide, Installation Guide, Elise3, TD 92679GB.

18 System 900 Interface

This chapter handles settings for the connection to the System 900 A-bus. When the A-bus is not connected, the bus operating mode should be set to 'No A-bus'. All other parameters only needs to be set when Unite CM is connected to a Central Unit in the System 900, or controlling the communication on the A-bus in systems without a Central Unit.

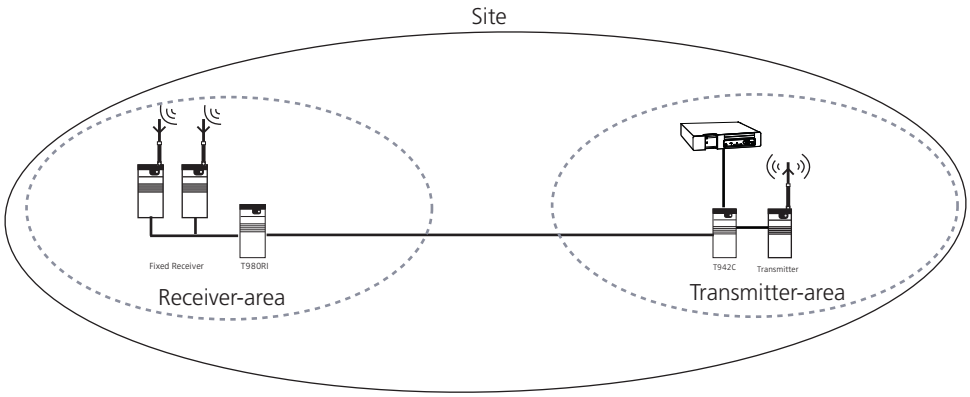


Figure 54. Modules connected to Unite CM via Central Unit.

Figure 54 illustrates a two-way system where the Transmitter and Receiver Interface are connected to the Unite CM via the Central Unit. This solution can be used in small system where the distance between the receiver-area and transmitter-area is short. Since a psychical trunk line is required between the Receiver Interface and the Central Unit, a short distance is preferred.

In this solution, the Unite CM acts as a slave on the A-bus since the Central Unit is used. The alarms, locations etc. received from the receiver-area are distributed via the Central Unit to the Unite CM. The Unite CM then distributes the alarms, locations etc. to an appropriate application.

In this solution, the basic parameters are as follows:

- Receiver Interface
  - "Number of modules to receive alarms" is set to "1" (NOTE: This parameter is set in the PCPAR application, see General Description PCPAR, TD 90799GB)

- Unite CM:
  - "Bus operating mode" is set to "Abus with central unit".
  - "Prefix and call number range" is set to the same prefix as in the Central Unit.
  - The destination for alarm, locations etc. received from the System 900 is set under "Message Distribution"; For example; 127.0.0.1/BasicAlarmHandler.

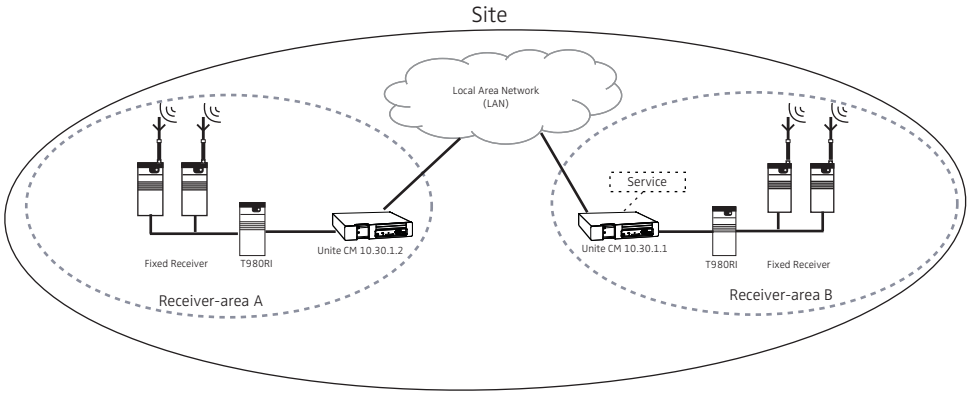


Figure 55. Connection without Central Unit in an One-way system

Figure 55 illustrates an one-way system where the Receiver Interfaces are connected directly to the A-bus of the Unite CMs. The solution can be used in large systems with several receiver-areas and where no Central Unit is to be used. The alarms, locations etc. received from receiver-area A are distributed over IP to the receiver-area B where the Unite CM is located. This Unite CM distributes the alarms, locations etc. to the applicable service.

In this solution, the basic parameters are as follows:

- Receiver Interface
  - "Number of modules to receive alarms" is set to "1" (NOTE: This parameter is set in the PCPAR application, see General Description PCPAR, TD 90799GB)

- Unite CM on Receiver-area A:
  - "Bus operating mode" is set to "Abus without central unit".
  - The destination for alarm, locations etc. received from the System 900 is set under "Message Distribution". For example; 10.30.1.1/BasicAlarmHandler. Note that the destination is the Unite CM on Receiver-area B.

- Unite CM on Receiver-area B:
  - "Bus operating mode" is set to "Abus without central unit".
  - The destination for alarm, locations etc. received from the System 900 is set under "Message Distribution"; For example; 127.0.0.1/BasicAlarmHandler.

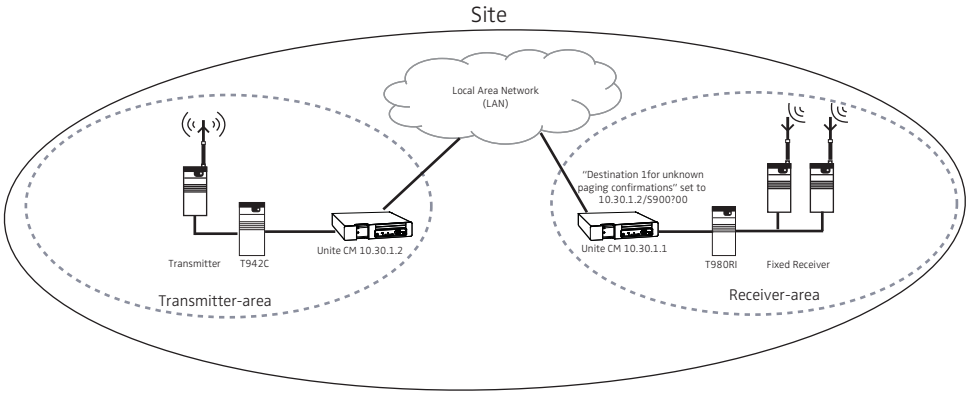


Figure 56. Two-way paging system

In Figure 56, the Receiver Interface is connected directly to the A-bus of the Unite CM on the receiving-area. In a system where it is required that a user of a handset manually shall acknowledge of a paging, the Unite CM on the receiver-area must distribute the acknowledgment to the Unite CM on the transmitter-area, where also the Central Unit is located.

In this solution, the basic parameters are as follows:

- Receiver Interface
  - "Number of modules to receive alarms" is set to "1" (NOTE: This parameter is set in the PCPAR application, see General Description PCPAR, TD 90799GB)

- Unite CM on the Receiver-area:
  - "Bus operating mode" is set to "Abus without central unit".
  - "Prefix and call number range" is set to the same prefix as in the Central Unit.
  - "Destination 1 for unknown paging confirmations" is set to the Unite address of the Central Unit; for example 10.30.1.2/S900?00.
  - The corresponding destination for alarm, locations etc. received from the System 900 is set under "Message Distribution"

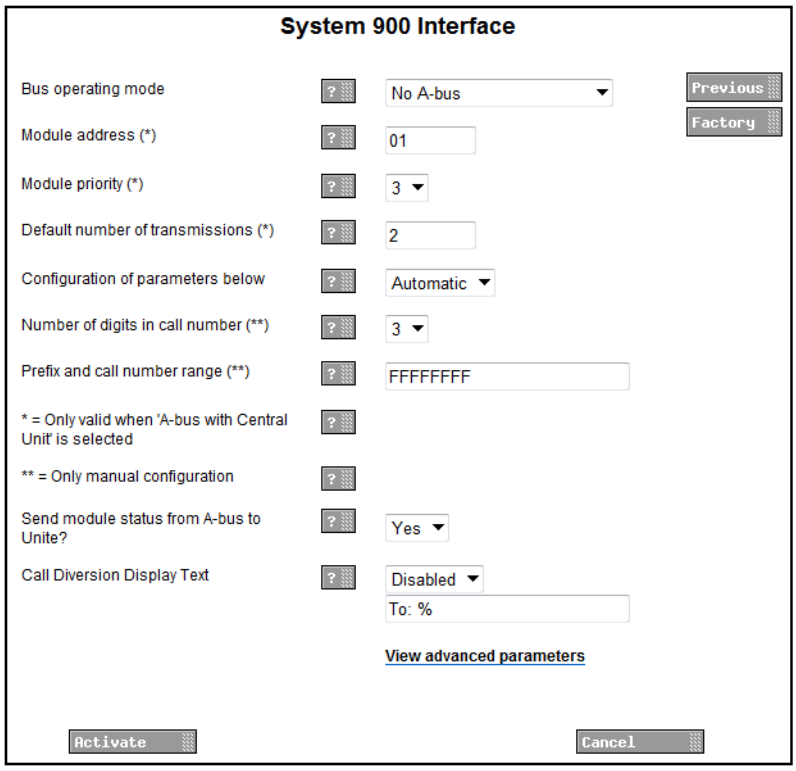
- Unite CM on the Transmitter-area:
  - "Bus operating mode" is set to "Abus with central unit".
  - "Prefix and call number range" is set to the same prefix as in the Central Unit.

18.1 System 900 Configuration Page

1 Click ‘‘Configuration’’ on the start page.

2 Select Other > Advanced Configuration in the menu on the *Configuration* page.

3 Click ''System 900'' under 900 Interface, in the menu on the *Advanced Configuration* page.



4 Enter/select the following settings:

- Bus operating mode
  - A-bus with Central Unit: Unite CM is connected to a system with a Central Unit. If Unite CM expects an A-bus with Central Unit, Unite CM will indicate ''application problem''.
  - A-bus without Central Unit: Unite CM controls the communication on the A-bus. This option can for example be used if you want to connect the Receiver Interface T980RI directly to the Unite CM's A-bus.
  - No A-bus connected: The A-bus connection is not used.

- Module Address

  This is the A-bus module address used when Unite CM is connected to a system with a Central Unit.
- Module priority

  This is the Unite CM priority on the A-bus. This parameter is only used when Unite CM is connected to an A-bus with Central Unit.
- Default number of transmissions

  This is how many times a paging is transmitted in the System 900. This parameter is only used when Unite CM is connected to an A-bus with Central Unit.
- Automatic or Manual configuration of prefix and call number

  When Unite CM is connected to an A-bus with Central Unit, the parameters in the Central Unit can be used and this parameter can be set to ''automatic''. If Unite CM is controlling the communication on the A-bus, the parameters have to be configured manually.
- Number of digits in call number

  This is the number of digits in the handset addresses in the system. If Unite CM is controlling the communication on the A-bus, this parameter has to be set manually.

- Prefix and call number range

  This is the prefix that is used in the system. The prefix has to be the same as for the other modules in the system. If Unite CM is controlling the communication on the A-bus, this parameter has to be set manually.
- Send module status from A-bus to Unite

  When this parameter is enabled, Unite CM sends module status to Unite as a status log.
- Call Diversion Display Text

  When this parameter is enabled, the text specified is added to the display message when a call diversion takes place. The original Call ID can be included in the parameter text by writing a % character where the Call ID shall be inserted.

5 Click ''Activate''.

18.1.1 Advanced parameters in System 900 interface

Additional parameters for the System 900 can be set if needed.

1 Click ''Configuration'' on the start page.

2 Select Other > Advanced Configuration in the menu on the *Configuration* page.

3 Click ''System 900'' under 900 Interface, in the menu on the *Advanced Configuration* page.

4 Click "View advanced parameters."

- Priority Transmissions 1- 9

  This parameter determines the number of message transmissions for pagings with priorities 1 to 9. Default is to use the value defined by parameter *Default number of transmissions*.
- Set Beep at each transmission (TX) for same paging ID

  The parameter is normally set when sending a paging with identical id as a previously sent paging.
- Alarm user data

  User data in alarm block from Unite can be used as first location in alarm block to 900 system. This parameter makes it possible to disable the handling of alarm user data.
- Portable position

  Portable position (both 9d base and sign post location) in alarm and location block from Unite can be used as locations in alarm block to 900 system. This parameter makes it possible to disable the portable positions.
- 9d base of location

  9d base location in alarm and location block from Unite can be used as location in alarm block to 900 system. This parameter makes it possible to ignore the 9d base location if any signpost location exist.
- Use manual location type in location block

  Manual location data received in an alarm block from A-bus is set as location type '5' in the location block when sent to Unite when this parameter is set. Unset if manual location from A-bus shall not be sent as an location type (The manual location data is always set as 'Data' when converting A-bus alarm block to Unite).
- Block time for additional transmissions from same handset

  Additional alarms and/or messages with mobile data from A-bus can be blocked for a short time to avoid that a duplicate of the same alarm or mobile data transmission (i.e. from same transmitter) is sent to Unite. This parameter is useful if more than one

Receiver Interface can send messages from handset to the 900 interface. Time in seconds.

- Convert '*' and '#' in mobile data

  The '*' and '#' characters sent from 922 handset in mobile data is sent as 'B' and 'C' characters on A-bus. This parameter defines if the 'B' and 'C' characters received from A-bus should be sent as '*' and '#' on Unite. It also means that '*' and '#' characters received from Unite in user key data is sent as 'B' and 'C' in the RI status block sent on A-bus. Set parameter to 'No' for transparent behaviour (no conversion).

- Remove leading zeros in call number from bus

  Set this parameter to 'No' if leading zeros in call number received from bus should be kept when sending to Unite. Call number would for example be set to 0012 instead of 12 if number of digits is 4 in system 900.

- Send pagings with unknown paging functions to Unite

  Set parameter to 'Yes' if this 900 interface shall send module status received from A-bus to Unite as system status blocks. This also means that this 900 interface will subscribe for module status from central unit if connected as slave.

- Carrier addressing mode on UNITE

  Set this parameter to 'Full' if system prefix should be kept for all call numbers handled from and to Unite (e.g. 3AADD100 instead of 100). No prefix is in that case added when an address is received from Unite and sent to A-bus. No prefix is removed for addresses received from A-bus and sent to Unite. If mode is set to 'Filtered', prefix is removed and only the call number is used when sending messages to and from Unite.

- Transparent mode for generic data

  Set this parameter to ''Yes'' if this 900 interface should send unknown generic data received in a mobile-to-base block from A-bus as mobile data on Unite. Generic data will have the string 'GD@' as prefix, i.e. generic data from A-bus containing '01020501' will be sent as mobile data 'GD@01020501' on Unite. With unknown generic data means everything that is not alarm or mobile data from portable. Generic data in paging will also be handled. If the body part of a paging text begins with prefix 'GD@', the 900 interface will remove the prefix and set remaining text as paging text when sending the paging to A-bus. The paging function will be set to 12, 'Generic data block from base'.

- Destination for unknown paging confirmations

  This parameter defines a Unite destination (i.e. IP-address/Service?ModuleAddress) to which the 900 interface will send any received manual acknowledge from bus that does not match a previous sent paging. If a RI-module is connected to a 900 interface running as master on bus, RI-module will send manual acknowledge from mobiles to the 900 interface. If the 900 interface can not find a previous sent paging with matching running number in queue, it can distribute this confirmation to another 900 interface that sends it on A-bus to the module address specified by the unite address (after the '?' char). It is usually address 00 (a central unit) that shall receive the manual acknowledge. Central unit will then send it to paging origin module on bus.

- Automatically send alarm acknowledge

  Set this parameter to ''Yes'' if this 900 interface shall send alarm acknowledge message to portables that request acknowledge for an alarm. Prox900 will then send alarm acknowledge when another application on Unite has accepted the alarm. Set parameter to ''No'' if the receiving application sends the alarm acknowledge message instead (probably by using the parameter for sending generic data through the 900 interface. An Alarm acknowledge would then be a paging back to portable with string 'GD@01020301' as text body).

- Paging priority for alarm acknowledge

  This parameter defines the paging priority for an alarm acknowledge sent by system 900 interface. Only valid if parameter 'Automatically send alarm acknowledge' is set to 'Yes'.

- Handle 'Attention' for Interactive Message

  The Unite specification for an Interactive Message includes a function called 'Attention' which specifies a time interval. If set in an Interactive Message, the receiving portable shall repeat the indication of the message with this interval until an option is selected by user. However, Interactive Message features are not supported by system 900 portables except for the parts that are common with standard paging. The system 900 interface can simulate the 'Attention' function by resending the paging to the central unit at the specified interval time. The paging will be repeated to the central unit for 15 minutes or until the 'Time To Live' specified in the message expires. Sending an Interactive Message with 'Attention' set will of course increase the traffic in the 900 system. Set this parameter to "No" to make the system 900 interface discard the repetition of pagings.
- Convert 'speech paging' from bus to standard paging

  This parameter defines if a speech or MTM paging received from A-bus shall be distributed to Unite as a call setup or as a standard paging. Speech and MTM pagings from A-bus can normally only be handled by system 900 pagers with speech capacity (e.g. 922 portables). A speech or MTM paging from A-bus should therefore only be sent as call setup if it shall be sent back to A-bus via another system 900 interface.
- Application sets 'running number'

  An application that sends messages to system 900 interface can determine what 'running number' to use on A-bus. This is done by setting Message ID to wanted 'running number'. This works for pagings, erase pagings and speech pagings received from Unite if the Unite address of the sending application is set in this parameter (i.e. 172.20.13.124/EventHandler). Message ID's in messages from other applications will not be used as 'running number', i.e the central unit sets 'running number' (default).

18.2 System 900 Message Distribution

The 900 Interface has distribution lists that define where incoming data from the handsets in the System 900 and the System 900 modules should be sent. The receivers are addressed in the same way as for the DECT or WLAN Interface that is described in Installation Guide, Elise3, TD 92679GB.

1 Click ''Configuration'' on the start page.

2 Select Other > Advanced Configuration in the menu on the *Configuration* page.

3 Click ''Messaging Distribution'' under 900 Interface in the menu on the *Advanced Configuration* page.

The following information is supported:

- Alarm
  - Personal alarms with location information from handsets.
- Mobile Data
  - Data sent from handsets.
- Input activity
  - An input on an Alarm Module has been activated.
- Location
  - Special Location[1] information from handsets.
- Availability Info
  - Includes absence information, that is if a handset is placed in Charging/Storage Rack.

Pagings that are received from the A-bus will be transmitted to the destination that corresponds to a Messaging User.

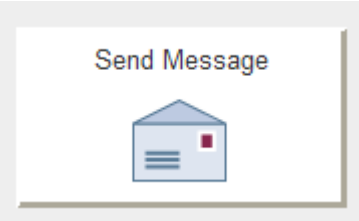
1. The Special Location can be sent every time a cordless phone gets a new location from a locator in the system. This requires configuration both in the handset and in the locator. Also called ''Immediate Alarm Transmission''.

19 Create and Send Messages

Creating and sending messages via the Messaging Tool requires no password and can be done by any user in the system. NetPage, on the other hand, can be configured to require a login, see 19.4.2 NetPage Configuration on page 151.

Depending on license, different tools for messaging are displayed:

- Messaging Tool - included if the license does not include NetPage
- NetPage - included in Unite CM Compact license, but an additional license is required for the Unite CM Enterprise license



19.1 Create and Send Messages via the Messaging Tool

The Messaging Tool GUI is displayed on Unite CMs without additional license.

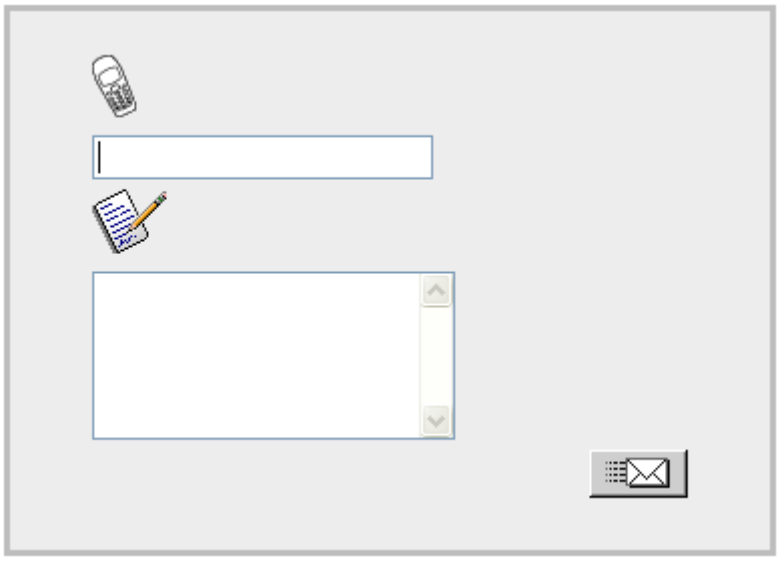


Figure 57. Messaging Tool GUI.

1 Click ‘‘Send Message’’ on the start page. The Message Tool opens.

2 Enter Call ID in the top text field.

3 Enter message in the bottom text field.

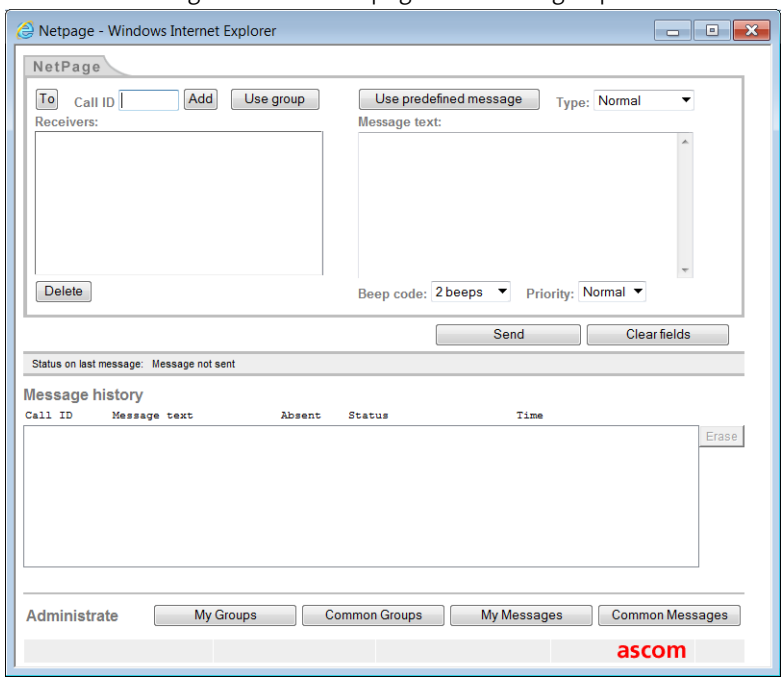
4 Click the send button. The message is sent to the receiver.

19.2 Create and Send Messages via NetPage

NOTE: Requires an additional license, see 1.1 Licenses for Unite CM on page 1.

NetPage supports messages with character encoding UTF-8 (for example Russian characters and Swedish characters)

1 Click ''Send Message'' on the start page. The NetPage opens.



2 Click either the ''To'' button to fetch number from the Users list or enter number in the *Call ID* field and click ''Add''. Several Call IDs can be added.

If the message shall be sent to a group click the ''Use group'' button, select group and click ''OK''.

3 Enter message text in the *Message* text field or click ''Use predefined message'', select a message in the list and click ''OK''.

4 Click ''Send''.

19.2.1 Predefined Messages

NOTE: This feature can only be reached from index4, that is the default NetPage GUI.

The predefined messages include message text, beep characteristics, priority and message type. There are two types of messages: ''Common Messages'' and ''My Messages''.

NOTE: The maximum message length differs depending on which system or handset the message is sent to and the amount of special characters included in the message.

Common Messages

Common Messages can be used by all NetPage users. Up to 30 ''Common Messages'' can be created. These messages are stored on Unite CM and can only be changed by authorized persons.

My Messages

Up to 30 predefined ''My Messages'' with 120 characters per message can be created. It is also possible to have fewer ''My Messages'' containing more characters. These messages are stored locally and can only be accessed or changed from that PC.

19.2.2 Create a Predefined Message

1 Click the ''Common Messages'' or ''My Messages'' button in NetPage. For ''Common Messages'' enter the user name ''user'' and the password ''password''.

2 Click ''Add message''.

3 Enter the name of the message and add a message text of maximum 250 characters.

4 Set the message type, beep signal and priority.

5 Click ''Save''.

6 Click ''Close'' to exit the administration.

19.2.3 Edit a Predefined Message

1 Click the ''Common Messages'' or ''My Messages'' button in NetPage. For ''Common Messages'' enter user name and password (default ''user'' and ''password'').

2 Click the message that shall be changed.

3 Make the changes and click ''Save''.

4 Click ''Close'' to exit the administration.

19.2.4 Message History Status

Status on the last sent message:

Status	Description
Message accepted:	The message is accepted by NetPage and will be transmitted.
Message completed:	The Messaging System has completed the transmission of the message.

In the default user interface (index4), other ''message history statuses'' can appear such as:

- The time and date a message was delivered
- Call Diversion
- Manual Acknowledge
- Delivery Receipt
- Absence

  NOTE: A handset that is offline[1] will normally not be indicated as absent. Instead, the status *Fail* will be shown. However, the Unite CM can treat the handset as absent even when it is offline (see 15.4.3 Absence Status for Offline Devices on page 132). In that case the handset will also be indicated as absent in the Message history field.

19.3 My Groups

NOTE: ''My Groups'' are created from the NetPage and are not to be mistaken for the groups created from the Configuration page in Unite CM. This functionality is only accessible

1."Offline" means that the handset is logged out, out of range, turned off, or out of battery.

from index4, see figure 78 on page 177.

''My Groups'' are stored locally and can only be accessed or changed from the PC where they are stored.

There is a limited storage area. This means that, for groups with approximately 20 characters (name and Call ID), the following applies:

Amount of Groups	Group Members
10	19
15	7
20	2

19.3.1 Create Groups

1 Click ''My groups'' button in NetPage.

2 Click ''Add group''.

3 Enter a name for the group in the Name text field.

4 Click the ''To'' button and select users (from the phonebook) to be members of this group or enter number in the Call ID text field and click ''Add''.

5 Click ''Save''.

6 Click ''Close'' to exit the administration.

19.3.2 Edit Groups

1 Click ''My groups'' button in NetPage.

2 Click the group that should be changed.

3 Make changes and click ''Save''.

4 Click ''Close'' to exit the administration.

19.4 Additional Messaging Configuration

NOTE: Requires ''admin'' or ''sysadmin'' password, see chapter 3 General on page 14.

The operation of the messaging tools is described in 19.1 Create and Send Messages via the Messaging Tool on page 147.

19.4.1 Messaging Tool Configuration

It is possible to change the title of the Messaging Tool web page.

1 Click ''Configuration'' on the start page.

2 Select Other > Advanced Configuration in the menu on the *Configuration* page.

3 Click ''Messaging Tool'' in the menu on *Advanced Configuration* page.

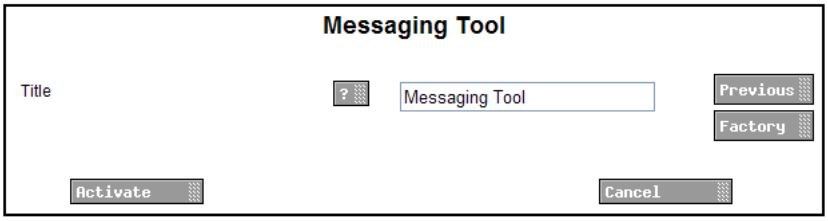


Figure 58. The Messaging Tool page.

4 Enter text to be shown as title. Click ''Activate''.

19.4.2 NetPage Configuration

Configure NetPage messaging

The following settings are applicable for NetPage web messaging.

To set messaging properties:

1 Click ''Configuration'' on the start page.

2 Select Other > Advanced Configuration in the menu on *Configuration* page.

3 Select ''Web Messaging'' in the menu on *Advanced Configuration* page.

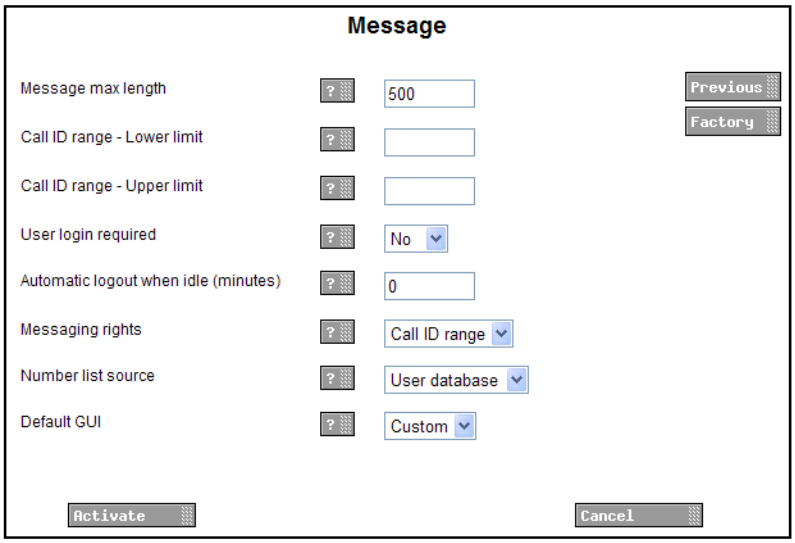


Figure 59. The Message page.

4 Enter values for messaging.

The following parameter can be set:

- Message max length.
  Sets the maximum number of characters that can be forwarded to a unit. Messages longer than the set value are truncated.
- Call ID range - Lower limit
  Sets the lower limit of a Call ID range. Messages sent to Call IDs out of this range are cancelled. An empty field means no lower limit.

- Call ID range - Upper limit
  Sets the upper limit of a Call ID range. Messages sent to Call IDs out of this range are cancelled. An empty field means no upper limit.

  User login required
  Sets whether a login is required for NetPage. If set, only configured users can login to NetPage. This parameter will only have effect on the default GUI (index4).
- Automatic logout when idle (minutes)
  Sets how long a user can be idle before being logged out. To prevent automatic logout, leave this field empty. If the parameter ''User login required'' is set to ''No'', leave this field empty.
- Messaging rights. Choose between Call ID range and User rights to determine how NetPage shall verify Call IDs.
  ''Call ID range'' means that Call IDs are verified according to the Call ID range limit settings.
  ''User rights'' means that Call IDs are verified according to the messaging rights defined for the user. This requires that the parameter ''User login required'' is set to ''Yes''.
- Number list source. Choose between File (FTP area) and User database.
- Default GUI. Select which GUI to use as start page for NetPage. Choose between Custom, Index 1, Index 2, Index 3, Index 4. See 22.2 Customize the User Interface (GUI) on page 170 for more information about the different GUI's.

5 Click ''Activate''.

Creating or Updating the Number list

In the NetPage default GUI (index.html), a number list can be accessed by clicking the ''Search'' button. The number list can be created from either an uploaded CSV file or from the number plan used by Unite CM. Before the number list can be used, the entries have to be added.

The number list entries can be created from any CSV file, using Microsoft Excel or any leading spreadsheet or relational database application.

NOTE: The parameter ''Number list source'' must be set to ''File (FTP area)'' if number list shall be created from uploaded CSV file. See 19.4.2 NetPage Configuration on page 151.

The CSV file is uploaded/pasted with the ''Number list upload'' program (included in NetPage) as described below.

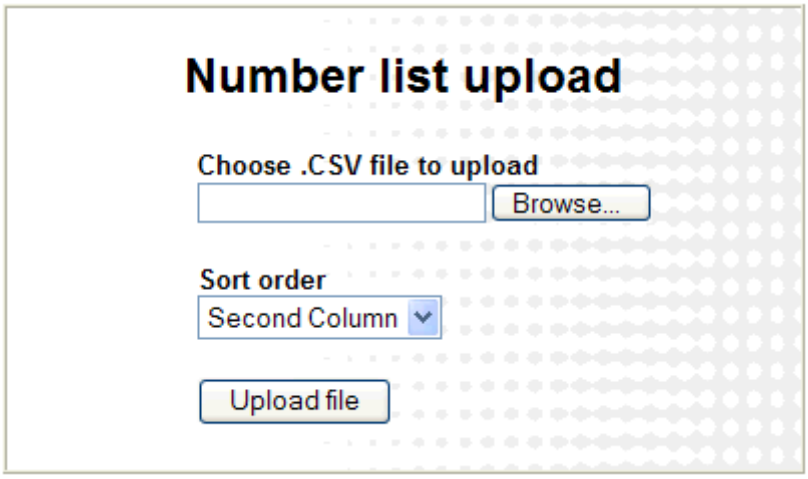


Figure 60. The page for uploading a new or updated CSV file.

1 Create a CSV file with the following format:

First name 1;Surname 1;Telephone number 1

First name 2;Surname 2;Telephone number 2

2 Open the page: http://xxx.xxx.xxx.xxx/admin/user/uploadnrlist.html.
Log on with ''user''. The default password is ''password''.
The application shown in Figure 60 will appear.

3 Browse to find the CSV file. Choose the sort order. Click ''Upload file''.

When the CSV file is uploaded, it will be converted and saved as ''uploadednrlist.js''. The file is a text file with the following format:

nr_array=[[''First name 1'',''Surname 1'',''Telephone number 1''],[''First name 2'', ''Surname 2'',''Telephone number 2'']];

If you later want to edit the number list, the ''uploadednrlist.js'' file is accessible with the FTP client and can also be modified manually.

4 Test that the number list works as desired.

5 Make a backup of the ''uploadednrlist.js'' file, see further in 19.4.4 Backup and Restore of NetPage files on page 154.

NOTE: When the phonebook has been updated, be sure to clear the cache memory on the web browser.

19.4.3 Colored messaging

It is possible to add color information in messages sent to handsets. The beep code in a message is mapped to a color. When this feature is enabled, color information will be added to all transmitted messages.

NOTE: This feature is only applicable for DECT and WLAN.

1 Click ''Configuration'' on the start page.

2 Click Other > Advanced Configuration in the menu on the *Configuration* page.

3 Click ''Coloured Messaging'' in the menu on the *Advanced Configuration* page.

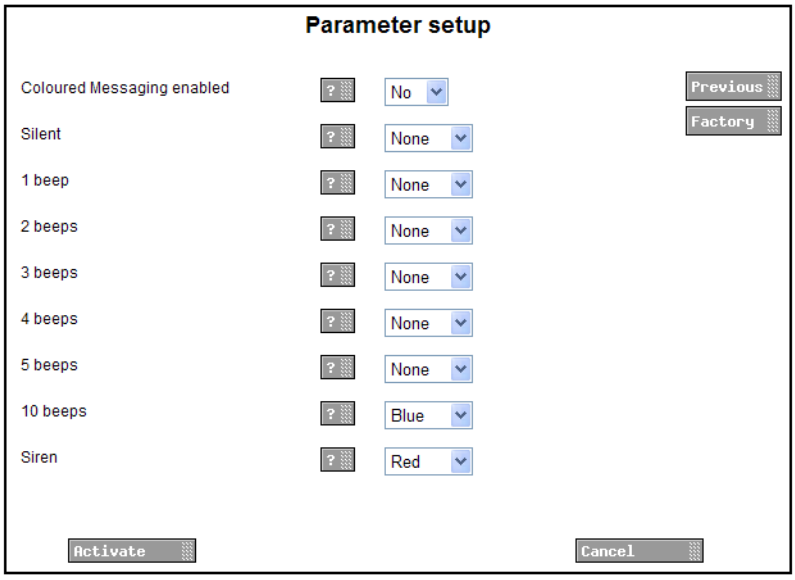


Figure 61. The Coloured Messaging page.

4 Set Coloured Messaging enabled to ''Yes'' or ''No''.

5 Map which colors that shall correspond to the different beep codes. These colors are displayed with messages in the handsets.

6 Click ''Activate''.

19.4.4 Backup and Restore of NetPage files

It is recommended to make a backup of all NetPage files, the phonebook and predefined groups and messages, if for example, you want to move a customized GUI to another module.

NetPage Files

NetPage files are the number list, the GUI files including image files and the Common Groups and the Common Messages files.

Backup

Copy and save modified files in the NetPage FTP area, see 22.2.2 Files for Translation/ Editing on page 171.

Restore

1 Put copies of the backup files in the NetPage FTP area, see 22.2.2 Files for Translation/Editing on page 171.

2 Test that NetPage is functioning properly, see 22.3 Test the New User Interface on page 178.

Backup of Predefined Groups and Messages

NOTE: Default user name is ''user'' and password is ''password'', but this can have been changed in your system.

Backup

1 Open NetPage. In the Administrate field, select the ''My Groups'' button. Click the ''Backup/ Restore'' button. The ''Backup/ Restore'' view is opened. Click ''Backup'' > ''Save''. Choose the file name and save.

2 Repeat the same process as above in point 1) but for ''My Messages''

Common messages are included in the ordinary backup for Unite CM. To backup common messages separately, repeat the same process as above in point 1) but for ''Common Messages''. (Log in with ''user'' and password ''password''.)

Restore

1 Open NetPage. In the Administrate field select the ''My Groups'' button. Click the ''Backup/ Restore'' button. In the ''Backup/ Restore'' view click ''Browse...'' and browse to the once backed-up file. Click Open > Restore.

2 Repeat the same process as above in point 1) but for ''My Messages''

3 If not already done, repeat the same process as above in point 1) but for ''Common Messages''. (Log on with ''user'' and password ''password''.)

4 Test that NetPage is functioning properly, see 22.3 Test the New User Interface on page 178.

20 Messaging Administration

All administration of Users, Groups, User Teams, Work shifts and Categories is done on the *Configuration* page under Messaging.

20.1 Users

All administration of the messaging users in the system is done under *Messaging* on the *Configuration* page.

For adding a new messaging user, see chapter 4.1 Add Users to Unite CM on page 20.

Symbols in Users

Edit a User, Group, Team, Work shift or a Diversion condition

Editing symbols:

Save changes for the edited user only

Discard changes

Edit additional User settings, such as giving a user a User ID and password for logging in or adding the user to a User Team.

Diversion exists

Diversion symbols:

Primary destination

Secondary destination

Destination enabled

Add a condition

Delete a condition/destination

Absent diversion

Not reachable diversion

Out of range diversion

Delete user

20.1.1 View Users

1 Click Messaging > Users in the menu on the *Configuration* page.

The Users page gives an overview of all users. For each user, Call IDs, categories and diversion are shown.

Search Users

You can search by last name, first name or Call ID. Then enter the first letter(s) or (number(s) and click ''Search''.

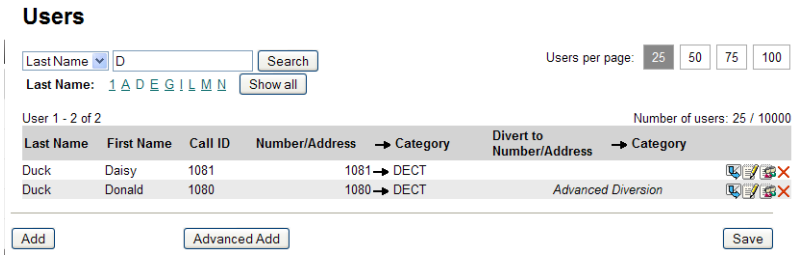


Figure 62. Search list of users where the last name begins with a D.

Change Users per page

When the Users page opens it will always show 25 users per page. The opened page can be changed and show 50, 75 or 100 users per page by clicking the desired value in the upper right corner.

20.1.2 Edit Users

1 Click Messaging > Users in the menu on the *Configuration* page.

2 Click the icon to the right of the user you want to edit.

The user settings can now be changed.

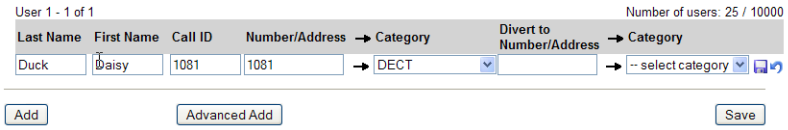


Figure 63. Edit a User

For changing the individual password, see chapter 4.2 Additional User Settings on page 23.

3 Click the '' '' symbol to the right of the user to save changes for this user only.

Use the ''Save'' button to save all users if many users are edited.

20.1.3 Delete Users

1 Click Messaging > Users in the menu on the *Configuration* page.

2 Click the ✕ icon to the right of the user you want to delete.

20.2 Groups

For adding a new group, see chapter 4.3 Create Groups on page 30.

Symbols used in Group Handling

Symbol	Description
	Group ID
	Broadcast ID
	Multicast group ID
	Handset added but not yet programmed
	Unsuccessful programming
	Handset removed from group but not yet programmed
	Unprogrammed members
	Activation of one/several members failed
	Activation of group failed - carrier interface problem
	Edit a Group
	Delete a Group

20.2.1 View Groups

1 Click Messaging > Groups in the menu on the *Configuration* page.

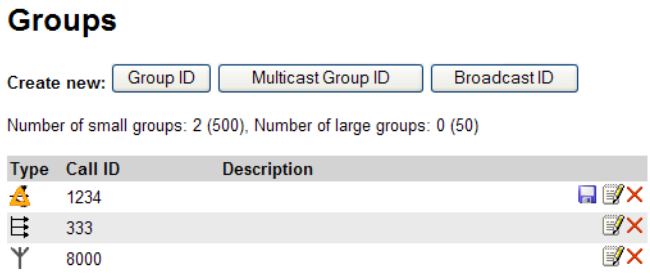


Figure 64. The Groups page.

The Groups page gives an overview of set up groups. For each group, Call IDs and additional Description is shown.

20.2.2 Edit Group

To edit a group:

In the Groups page, click the icon for the corresponding group.

20.2.3 Delete Group

1 Click Messaging > Groups in the menu on the *Configuration* page.

2 Click the ✕ icon to the right of the group you want to delete.

20.3 User Teams

For adding a user to a User Team and creating a User Team, see chapter Add Members to a User Team on page 34 and 4.4 Create User Teams on page 34.

Symbols used in User Teams

Symbol	Description
	Edit the User Team
	View all members included in the User Team
	Delete the User Team

20.3.1 Show Members of a User Team

1 Click Messaging > Teams in the menu on the *Configuration* page.

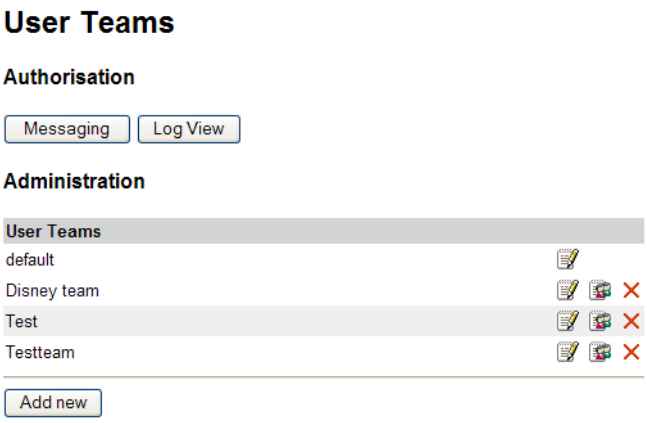


Figure 65. The Authorisation page for User Teams.

2 Click the symbol to the right of a User Team to see which members that are assigned to a specific User Team. Assignment is handled from the Users pages, see Add Members to a User Team on page 34 for more information.

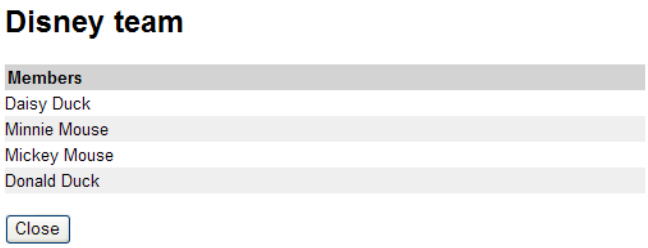


Figure 66. Showing members of the "Disney team".

20.3.2 Edit Messaging Rights

In the Messaging page, it is possible to edit authorities for the User Teams. These settings limit the number of addresses that are displayed in for example Netpage.

1 Click Messaging > Teams in the menu on the *Configuration* page.

2 Click ''Messaging'' under Authorisation.

Figure 67. The Messaging page.

Add Messaging Rights

1 Select one or more User Team check boxes and select from the drop-down list which User Team they should be able to send message to.

2 Click ''Add''.

3 Click ''Close'' when finished.

Remove Messaging Rights

1 Select one or more User Team check boxes and select from the drop-down list which User Team that should be removed.

2 Click ''Remove''.

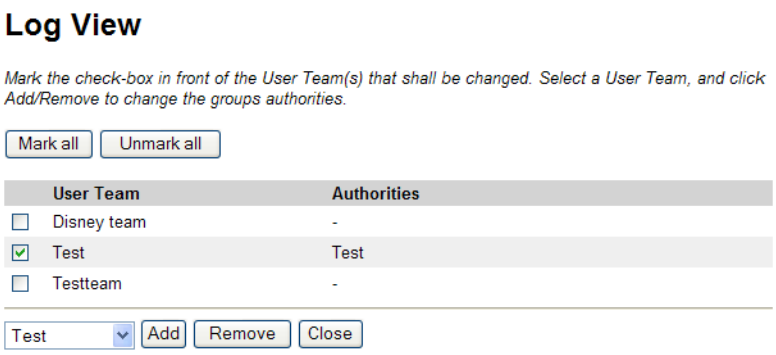
3 Click ''Close'' when finished.

20.3.3 Edit Log View Rights

In the Log View page, it is possible to edit the authorities for the User Teams. These settings restrict which activity logs that will be shown to the user in the Activity Log Viewer and can also be used to restrict which activities that are exported to a specified destination.

1 Click Messaging > Teams in the menu on the *Configuration* page.

2 Click ''Log View'' on the User Teams page.



Adding or removing log view rights is done in the same way as in messaging rights, see 20.3.2 Edit Messaging Rights.

20.3.4 Edit or Delete a User Team

1 Click Messaging > Teams in the menu on the *Configuration* page.

- Edit:

1 Click the symbol to the right of the User Team you want to edit.

2 Make your changes and click "Save".

- Delete:

1 Click the symbol to the right of the User Team you want to delete.

20.4 Work Shifts

For creating a Work Shift see 4.5 Create Work Shifts on page 34.

Symbols used in Work Shifts

Symbol	Description
	Edit the Work shift
	Delete the Work shift

20.4.1 Edit or Delete a work Shift

1 Click Messaging > Work shifts in the menu on the *Configuration* page.

- Edit:

1 Click the symbol to the right of the Work shift you want to.

2 Make your changes and click "Save".

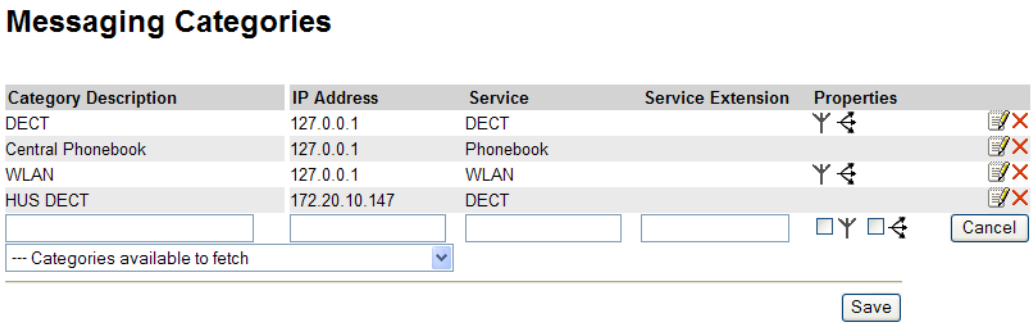
- Delete:

1 Click the symbol to the right of the Work shift you want to delete.

20.5 Add Messaging Category

1 Click "Users & Groups" on the start page.

2 Select Messaging > Categories in the menu on the *Configuration* page.



3 Enter the following settings:

Setting	Description

Category description:	Description of the category (will be shown in the configuration). Added automatically if the category is selected in the ''Category available to fetch'' drop-down list.
IP Address:	The IP address of the module that should handle messaging in the category. Added automatically if the category is selected in the ''Category available to fetch'' drop-down list.
Service:	The service on the module that handles the message. The name of the service running on a module is found in the System Overview page if the module is surveyed.
Service Extension: (optional)	Optional addressing information. For example used to add System 900 category information, where the Service Extension is set to ''category=X'', X represents the System 900 category A to J.
Properties:	Broadcast ( ) and Multicast ( ) can be selected if the category has any of those capabilities.

4 Click ''Save''.

20.5.1 Edit or Delete a Category

1 Click Messaging > Categories on the *Configuration* page.

- Edit:

1 Click the symbol to the right of the Category you want to edit.

2 Make your changes and click ''Save''.

- Delete:

1 Click the symbol to the right of the Category you want to delete.

20.6 Add S900 Composite Category for Multi-Site Paging

It is possible to map several S900 sites to one and same composite category, where each S900 site is represented by an IP-address. The composite category can be used for an S900 paging handset that moves between several sites.

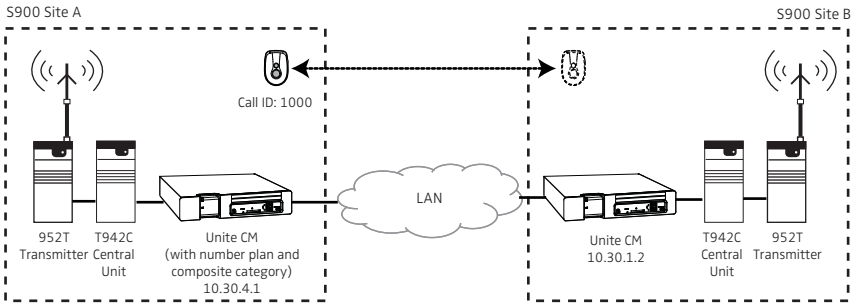
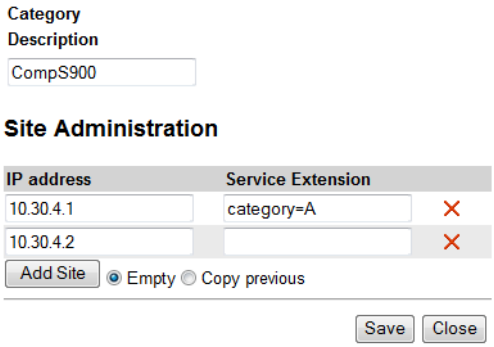


Figure 68. Example of a paging handset that is used on several sites.

As shown in Figure 68, the composite category is configured on the Unite CM that holds the number plan. The composite category is configured with the IP-addresses to the Unite CMs located on each site. The paging handset (Call ID 1000) is added as messaging user mapped to the composite category. This configuration makes it possible for a user of the paging handset to receive messages on both sites.

1 Click Messaging > Composite Categories on the *Configuration* page.

2 Click "Add new category".



3 In the *Category description* text field, enter the description of the composite category (will also be shown under Messaging Categories).

4 Click "Add Site".

5 In the *IP address* text field, enter the IP-address of the Unite CM located on the S900 site to be included in the composite category. Maximum nine S900 sites can be added to a composite category.

6 If needed, in the *Service Extension* text field, enter optional addressing information. For example System 900 category information, where the Service Extension is set to ''category=X'', X represents the System 900 category A to J.

7 If needed, repeat steps 4 — 5 to add additional IP address(es). Select "Copy Previous" if you want to copy the previous IP address.

8 Click "Save".

The composite category can now be mapped to an S900 messaging user, see 4.1.2 Add messaging users for paging on page 21.

20.6.1 Edit or Delete a Composite Category

1 Click Messaging > Composite Categories on the *Configuration* page.

- Edit:

1 Click the symbol to the right of the Category you want to edit.

2 Make your changes and click ''Save''.

- Delete:

1 Click the symbol to the right of the Category you want to delete.

21 Software Administration

Besides the software administration via Unite CM configuration page, it is also possible to administer the software via the module's Boot Mode GUI. This is described in the Installation Guide, Elise3, TD 92679GB. The Boot Mode GUI is typically used if no software is installed on the module or if it should be impossible to access the software.

21.1 Software Information

All information about the installed software is shown in this view. Two software versions can be installed on the module.

1 Click ''Configuration'' on the start page.

2 Select Software > Information in the menu on the *Configuration* page.

The software name, versions, the date they were installed and also which version that currently is running are shown.

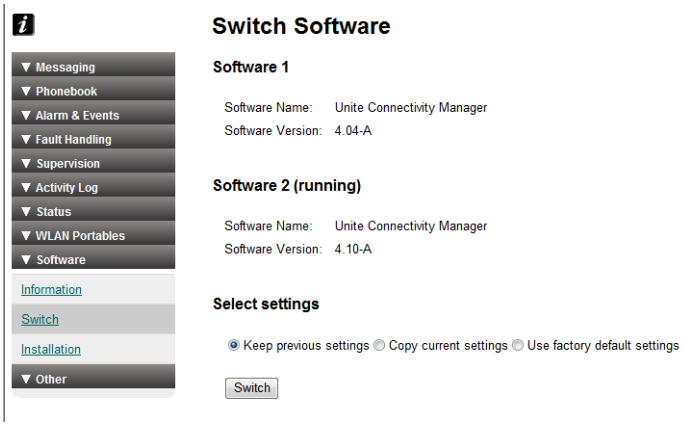
21.2 Switch Software

If two software versions are installed on the module you can switch between them.

NOTE: When switching software over a Remote Management Client (RMC) using previous settings, you might loose RMC connection to the module if the port is not opened on both software 1 and software 2.

1 Click ''Configuration'' on the start page.

2 Select Software > Switch in the menu on the *Configuration* page.



3 Under *Select settings*, select one of the following:

- Keep previous settings — means that the settings last used for the software is activated again after the switch. This option is only available if the software has been used at least one time before.
- Copy Current settings — means that you copy the configuration from the software you are currently using and is only available if both software are of the same type.
- Use factory default settings — means that you apply the default settings that were delivered from the factory.
  NOTE: The active software's current network settings will be kept and will also be applied to the software you want to switch to.

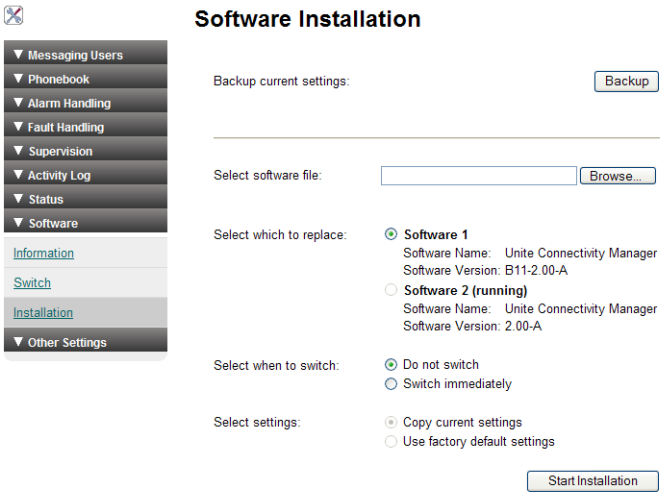
4 Click ''Switch''.

21.3 Install New Software

NOTE: It is not recommended to use the module's Management port when installing software.

1 Click ''Configuration'' on the start page.

2 Select Software > Installation in the menu on the *Configuration* page.



3 Select software (.pkg) to upload. The software will replace the not running software.

4 Select ''Switch immediately'' if you want to run the new software.

5 Select ''Copy current settings'' if you want the new software to inherit the settings currently used. This selection will have no effect if the software type is different than the currently used software. The module will always start up using factory settings if the software type differs.

6 Click the ''Start Installation'' button.

21.3.1 Install New Software in a Redundant System

When both the primary Unite CM and the secondary Unite CM are redundant, it is possible to install software on both Unite CMs simultaneously. It is only needed to install the software on the primary Unite CM since the software also will be installed on the secondary one automatically. Follow the instructions in 21.3 Install New Software on page 165.

21.3.2 Create a Software Backup

It is recommended to now and then create a backup of the software configuration.

1 Click ''Configuration'' on the start page.

2 Select Software > Installation in the menu on the *Configuration* page.

3 Click the ''Backup'' button.

Note that the backup will contain configuration for the running software only.

22 Administration of Language and User Interface

All text shown in the user interface is by default in English but a copy of the language can be translated and imported to Unite CM. Several languages can be added. The default English language is not possible to edit or remove. The supplied user interface can also be modified to suit the individual customer requirements concerning functionality.

Basic changes that can be made are:

- Translate or adapt text (see22.1.2 Translate/Edit the Language on page 168)
- Hide unused functionality (see 22.2.4 Change the NetPage User Interface Functionality on page 174)
- Modify the user interface to suit the customer's image (see 22.2 Customize the User Interface (GUI) on page 170)

NOTE: Unite CM user interface only supports the Latin-1 character set. However, the NetPage GUI also supports UTF-8 character set.

For the best screen appearance

Windows standard screen settings, using normal font size, are recommended. The recommended screen resolution is 1024 x 768.

How to edit

The code is thoroughly commented to make it easy to understand and can be edited with a simple text or HTML editor. Basic HTML, Java Script and CSS knowledge are recommended.

NOTE: Do not use an intelligent html editor like Frontpage or Dreamweaver, as it might corrupt the html code.

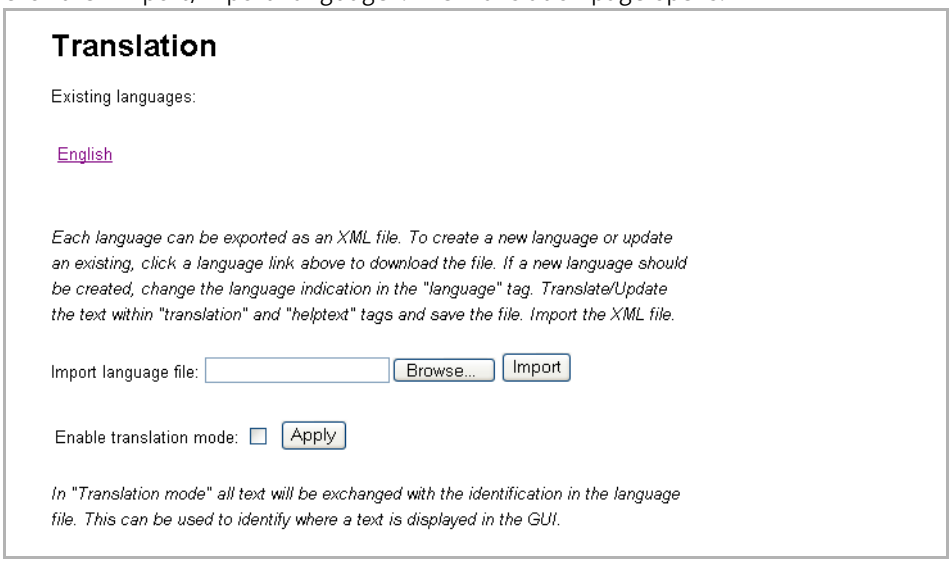
22.1 Customize the Language

22.1.1 Export a Language for Translation/Editing

1 Click ''Configuration'' on the start page.

2 Select Other > Set language in the menu on the *Configuration* page.

3 Click the ''Import/Export Language''. The Translation page opens.


Translation
Existing languages:
English
Each language can be exported as an XML file. To create a new language or update an existing, click a language link above to download the file. If a new language should be created, change the language indication in the "language" tag. Translate/Update the text within "translation" and "helptext" tags and save the file. Import the XML file.
Import language file:
Browse...
Import
Enable translation mode:
Apply
In "Translation mode" all text will be exchanged with the identification in the language file. This can be used to identify where a text is displayed in the GUI.

4 Click an existing language link to create or update languages. An XML file is generated from Unite CM and a File download window opens.

5 Save the file for translation or editing purposes. The file can be saved in any name during the translation.

22.1.2 Translate/Edit the Language

NOTE: This translation does not affect the NetPage GUI. If you want to translate the that GUI, see Example GUI index4 (default NetPage User Interface) on page 177.

In the downloaded language file, there are numerous tags but only the translation of two tags and one attribute are mandatory:

- <language id=''English''>
  the ''id'' attribute is the text that appears in the drop-down list
- <translation>
  text displayed in menus, on buttons, tabs etc.
- <helptext>
  on-line help text

Below is an example of a language file (just showing two buttons with helptext, for simplicity).

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<translations>
 <language id="English" type="complete">
  <app id="Alarm Manager">
   <text id="ACTION_TYPE_SELECTOR">
    <translation>Action Type</translation>
    <helptext>Select which type of action to take.</helptext>
   </text>
   <text id="ACTIVATE_EHCONF_OK">
    <translation>Activation of configuration OK.</translation>
   </text>
   <text id="ALARM_TYPE_SELECTOR">
    <translation>Alarm Type</translation>
    <helptext>The alarm type that should be triggered. </helptext>
   </text
  </app>
 </language>
</translations>
```

Figure 69. Example of a language file.

22.1.3 Show Pages in Translation Mode

All texts, buttons, menus etc. are identified with labels (for example TEXT_TRANSLATION_TITLE). With the translation mode function, it is possible to view the label for each button, menu etc. This can be helpful when translating the language file. For not losing one's bearings during the translation it is a help to open two windows and view one of them in translation mode and the other in normal mode.

1 Select the Enable translation mode check box in the Import/Export Language page and click ''Apply''.

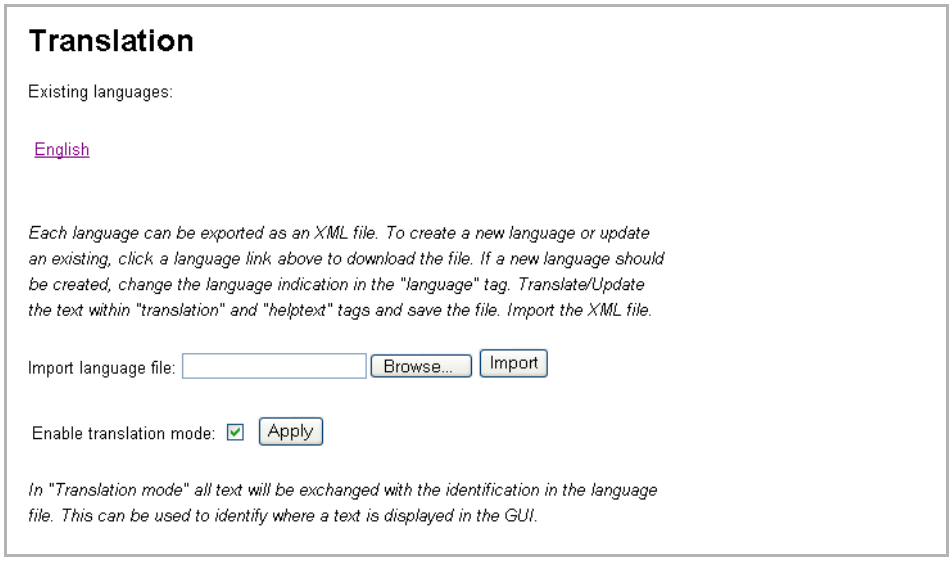

Translation
Existing languages:
English
Each language can be exported as an XML file. To create a new language or update an existing, click a language link above to download the file. If a new language should be created, change the language indication in the "language" tag. Translate/Update the text within "translation" and "helptext" tags and save the file. Import the XML file.
Import language file:
Browse...
Import
Enable translation mode:
Apply
In "Translation mode" all text will be exchanged with the identification in the language file. This can be used to identify where a text is displayed in the GUI.

Figure 70. Translation page in normal view.

All the labels on the pages are shown, see example below.

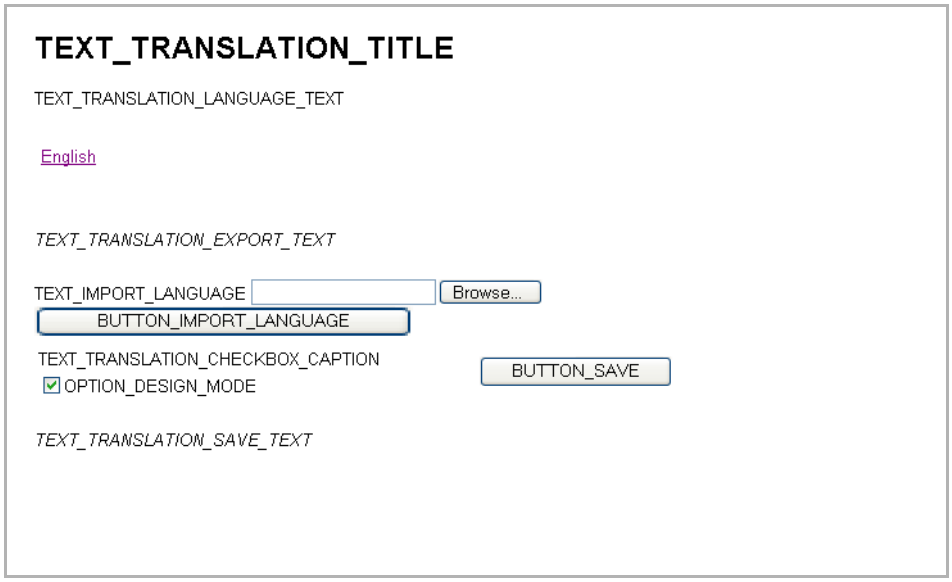


Figure 71. Translation page in translation mode.

To return to standard view:

1 Clear the OPTION_DESIGN_MODE check box.

2 Click ''BUTTON_SAVE''.

22.1.4 Import Language File for Unite CM

When the file is translated, it must be imported to Unite CM. Click ''Browse'' to locate the translated file and click the ''Import'' button.

The name of the translated language (the language ''id'' attribute) will appear as a link in the Existing Language list and can be downloaded for editing purposes.

22.1.5 Delete Language

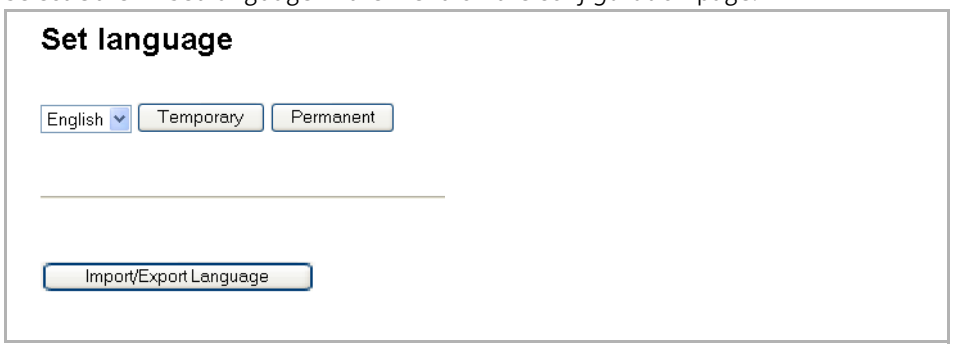
On the Translation page, click the ''Delete'' symbol to the right of the language you want to remove, see below. Note that it is not possible to remove the default language.

22.1.6 Select Language

Translated languages (the language ''id'' attribute) are shown together with the default language ''English'' in the language drop-down list in the Language page.

1 Click ''Configuration'' on the start page.

2 Select Other > Set language in the menu on the *Configuration* page.



3 Select language in the drop- down list and click ''Permanent''.

To change language for this session only, i.e. for this browser window until closed, click ''Temporary''.

22.2 Customize the User Interface (GUI)

Unite CM has an FTP area with default 50 MB disk space. The disk space can be set in the interval 5 MB up to 150 MB.

About 1.6 Mb of the disk space on the FTP area is dedicated for the NetPage user interfaces. The free space can be used for storing files and folders, for example, a customized user interface for sending messages.

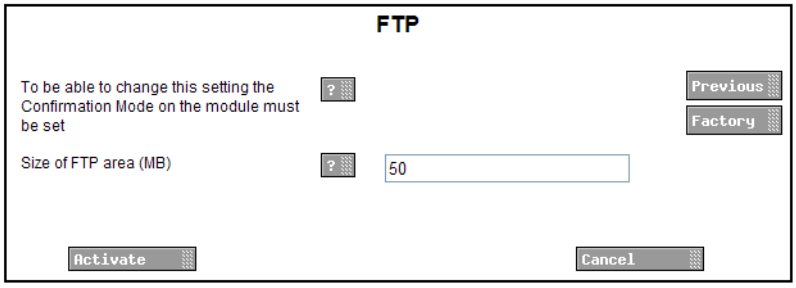
22.2.1 Change the Size of the FTP Area

This is a secured setting and before it can be activated it must manually be confirmed by pressing the mode button on the module.

1 Click ''Configuration'' on the start page.

2 Select Other > Advanced Configuration in the menu on the *Configuration* page.

3 Select FTP area under Common in the menu on the *Advanced Configuration* page.



4 Fill in required size between 5 – 150 MB and click ''Activate''.

5 Press the mode button on the module.

This is a secured setting so you will be prompt to confirm the change by pressing the mode button.

6 Click ''Activate'' to save the changes.

7 Click the mode button to return to normal mode immediately or wait 10 minutes for the module to return automatically. Any secured setting can be activated within the 10 minutes period.

The module needs to be restarted for the changes to take effect.

22.2.2 Files for Translation/Editing

1 Log on to Unite CM with an FTP client. Note that how to log on can differ between different FTP clients.[1]

Default username is ''ftpuser'' and default password is ''changemetoo''. xxx.xxx.xxx.xxx is the host name.

Examples:

- Windows Explorer: fill in ''ftp://username:password@xxx.xxx.xxx.xxx'' in the address field.
- Firefox: fill in ''ftp://xxx.xxx.xxx.xxx'' in the address field and log on with ''username'' and ''password''.

The files located in the Start page and Netpage folders, including GIFs and CSS, can be downloaded/copied to a folder on your hard disc.

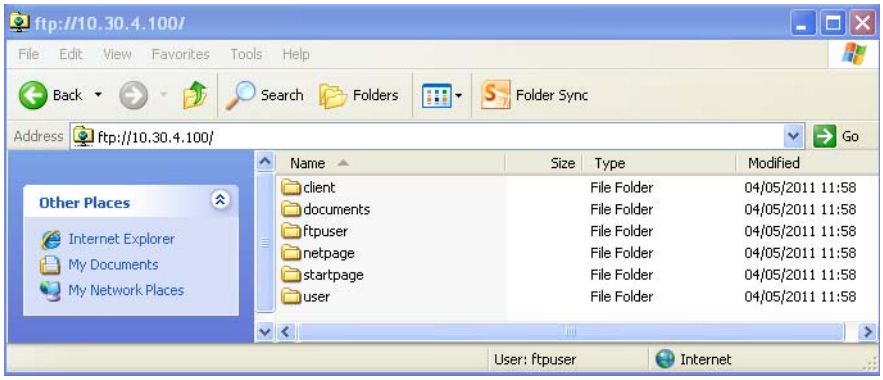


Figure 72. Folders on the FTP area

1.Internet Explorer is not an FTP client. It can be used for viewing but not for transferring files.

22.2.3 Default User Interfaces

Figure 73. Start page default user interface (index_template).

A copy of the default start page of Unite CM, see Figure 73 above, is stored in the start page folder on the FTP area of Unite CM. The start page index_template, is an html file which can be copied and edited. It is also possible to replace the start page with a completely new user interface.

When the edited or new html file is saved as index.html and placed in the Start page folder on the FTP area of Unite CM, it will replace the default start page.

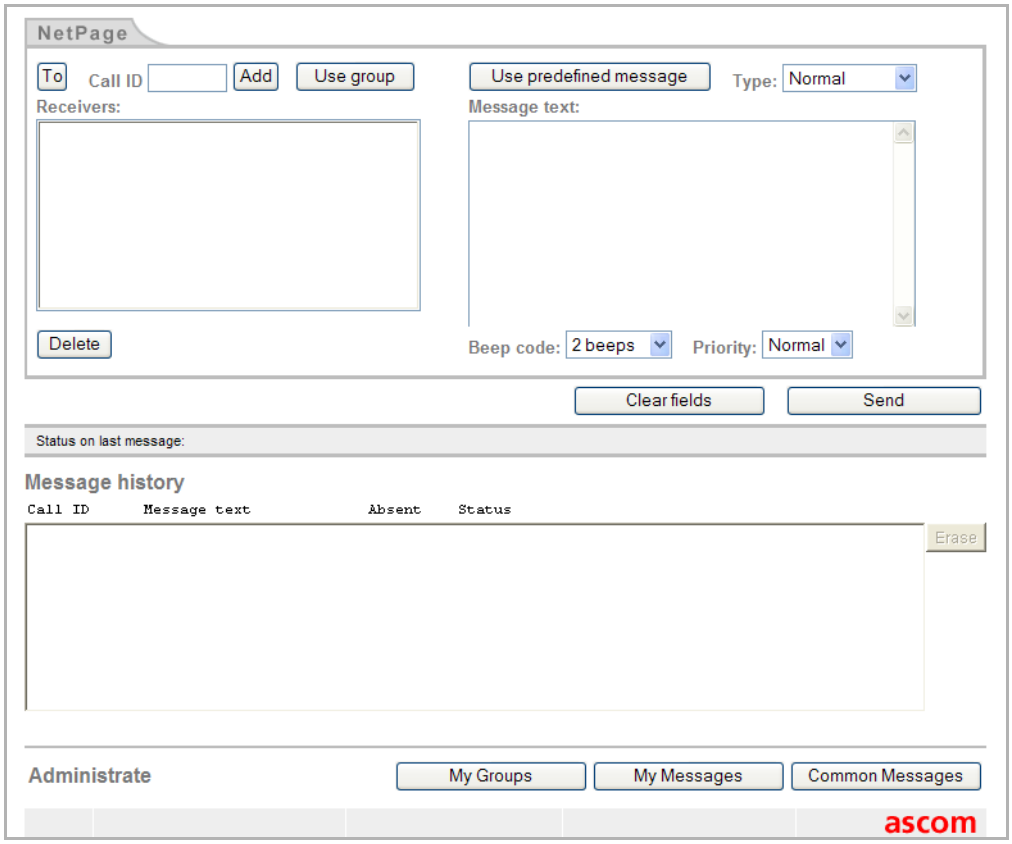


Figure 74. NetPage default user interface (index4).

The default NetPage user interface index.html, see figure 74 on page 172, opens from the start page by clicking ''Send Message''.

In the NetPage folder on the FTP area on Unite CM, there are four examples of the Netpage user interface, index1, index2, index3 and index4. Index4 is a copy of the default NetPage user interface.

All NetPage functionality is included in the default user interface (index), but all parameters that can be configured in the example user interfaces index1, index2 and index3, are not shown. The necessary code for viewing and configuring the hidden parameters is included, but they are marked as comments to prevent the browser from interpreting them, see Figure 76 and figure 77 on page 174.

The default user interface can be exchanged with one of the example user interfaces, shown in Figure 61, by saving the html file as index.html and replacing the existing index.html file.

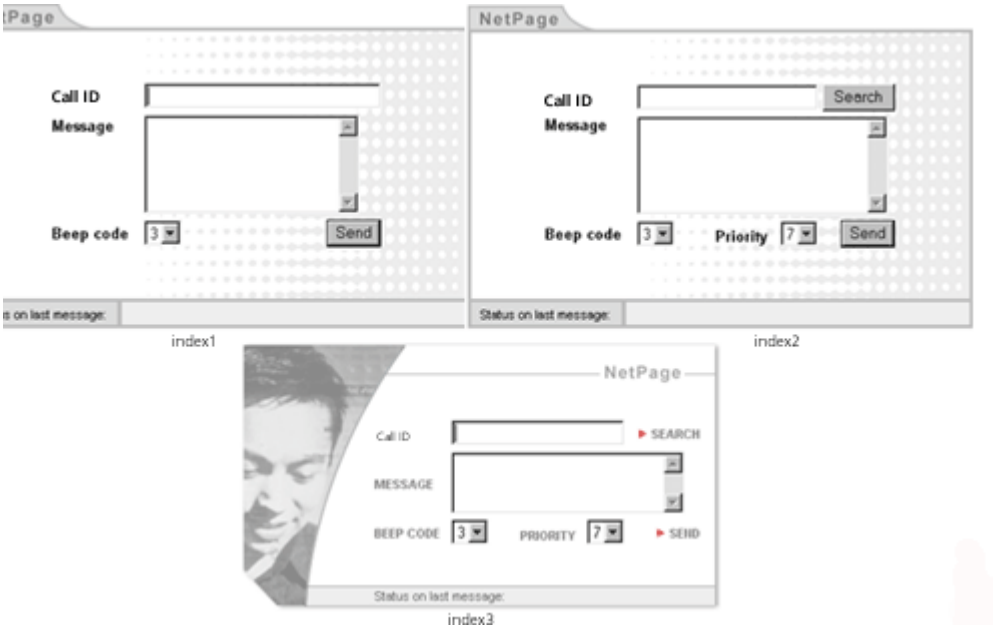


Figure 75. NetPage user interface examples; index1, index2 and index3.

NOTE: The JavaScript code in the HTML files is used for interpreting and displaying responses from the messaging system. It is recommended that this code is used unmodified, otherwise, the Message history functionality may be lost. Also, the Java Applets must be left unchanged to preserve the functionality.

NOTE: No server side scripts are allowed in the FTP area.

Priority and Beep Codes in the default NetPage User Interface

GUI Description	Priority Code
Low	9
Normal	7
High	3
Alarm[a]	1

a. Marked as hidden in the html page.

GUI Description	Beep Code
Silent	0
1 beep	1
2 beeps	2
3 beeps	3
4 beeps	4
5 beeps	5
10 beeps	6
Siren	7

22.2.4 Change the NetPage User Interface Functionality

As a help for locating comments/hidden text in the html code, the comment marks ''<!--'' and ''-->'' are used, see the example in Figure 76. The comment marks are also used to hide functionality in the user interface. Text written or functionality, framed by the comment marks are not interpreted by the web browser.

```
<TD valign="top" style="height:25">
<!--This is the button that opens the NetPage phonebook.
If the phonebook is not used, remove the complete script and
the    line (mark it as comments to be able to
include it again later on)-->
```

Figure 76. Example of how to mark html text as comments, i.e. hide it.

For comments included in the JavaScript code, the comment mark ''//'' is used, see Figure 77. Text written after the comment mark (in the same line) is not interpreted by the web browser.

```
function sendform() {
  addCallNo(document.testform.callno.value, '');
//If the user forgot to press 'add'
  tmplist = document.testform.callnolist;
```

Figure 77. Example on comments in a JavaScript.

Buttons, for example the ''To'' button that opens the NetPage phonebook, can also be hidden directly in the code. To do this, insert ''hidden'' (double quotation marks both before and after ''hidden'') as input type as follows:

```
document.write('<input type="button" value="...
```

will become

```
document.write('<input type="hidden" value="...
```

NOTE: To change the default user interface (index4) it is necessary to open and change one or more of the files: ''send.html'', ''receive.html'' and ''admin.html''.

NOTE: If changes to the phonebook access (''To'' button), beep codes or priority settings are made, it is also necessary to change the files ''editpagtext.html'' and ''leditpagtext.html'', to get a consistent user interface.

22.2.5 Creating a URL Call

It is also possible to send messages with hypertext links. This is useful in two ways. It makes it possible to open NetPage with some fields already filled in and to create buttons on another web page. For example, a hotel guest can then use a button on a computer screen to send a message to room service. In this case, NetPage is never shown to the user since the URL string contains all relevant data such as Call ID and message.

A CGI script on the NetPage web server is called with a set of parameters which are separated by the character ''&''. The ''immediate status'' (shown after the text ''Status on last message:'') can be presented on a separate web page by enclosing the URL to that web page. If no URL parameter is specified, the ''immediate status'' is always sent to the same web page as the message was generated from, and then that page has to handle the status. It is possible to use Common Groups when creating URL calls, Common Messages, My Groups and My Messages cannot be used.

NOTE: 1) The ''immediate status'' texts are shown in 22.2.6 Translation of the User Interfaces on page 176.
2) It is not possible to remote erase or receive ''message history status'' when using the URL call function.

The following parameters can be set for a URL message:

Description	Name	Value range	Default value
Call ID	no	-	-
Message text	msg	-	-
Message type	ack	0 no delivery receipt 1 delivery receipt 2 manual acknowledge	0
Beep code	bp	0-7	3
Priority	pri	1-9	7
Return page	url	-	Page you sent from
Message ID	id	see below	Set by NetPage
Erase message	del	see below	-
UTF8 encoded	utf8	see below	-

The wildcard ''*'' is allowed in the Call ID, for example Call IDs 9370-9379 can be written as 937*

NOTE: Wildcards are not supported by all systems.

Message ID

The Message ID is used to refer to previously sent messages, for example, to make the handset beep at each transmission of the message or to erase a previously sent message. The same Message ID as when the message originally was sent has to be used.

The Message ID can be set manually by the user or automatically by NetPage. NetPage sets the Message ID automatically if the parameter ''id'' is set to 0 or not specified. If the number is generated manually, it should be kept in the range 1 to 2147483647.

NOTE: NetPage does not check for conflicting manually set message IDs, therefore manually set message IDs must be kept unique. Conflicting message IDs will result in erroneous status reports among other problems.

Erase message

A previously sent message can be erased with a new URL call. Call ID, Message ID and the parameter ''del'' should be included in the URL call. This brings that the Message ID has to be set manually if a message should be able to erase later on. The parameter ''del'' has to be given a value but the value has no meaning, that is, it can have any value. The URL will look as follows, ''http://xxx.xxx.xxx.xxx/cgi-bin/npcgi?no=1234&id=23&del=1''.

UTF8 encoded

When NetPage is accessed from a cordless unit that uses WAP version earlier than 2.0, the message that is sent will be UTF8 encoded. The parameter ''utf8'' then has to be included to indicate this for the CGI script in NetPage. The parameter ''utf8'' has to be given a value but the value has no meaning, i.e. it can be any value.

NOTE: This parameter should not be used for HTML based NetPage applications.

22.2.6 Translation of the User Interfaces

The texts presented in the user interfaces can be translated. The translation is entered differently depending on the example user interface that is used. The HTML files index_template and index1, index2 and index3 are translated in the HTML code. The default Netpage user interface (index4) on the other hand is translated in the ''language.js'' and ''receive.html'' file, where receive.html includes the NetPage message history applet. See figure 64 on page 177 for an overview of where the different files are used.

Start Page

1 Download/copy the file and included images from the FTP area, see 22.2.2 Files for Translation/Editing on page 171.

2 Open the file in a text or HTML editor and translate all words.

3 Save the file.

4 Upload/paste the file to the FTP area, see 22.2.7 Upload the Files to the FTP Area on Unite CM on page 178.

5 Check that the user interface looks all right.

Example User Interfaces index_example1.html, index_example2.html and index_example3.html (NetPage GUI).

1 Download/copy the file and included images from the FTP area, see 22.2.2 Files for Translation/Editing on page 171.

2 Open the file in a text or HTML editor and translate all words and ''immediate status'' texts. For existing ''immediate status'' texts, see table below.

3 Save the file.

4 Upload/paste the file to the FTP area, see 22.2.7 Upload the Files to the FTP Area on Unite CM on page 178.

5 Check that the user interface looks all right.

NOTE: The parameter ''Default GUI'' must be set to ''Custom''. The parameter is found on the *Advanced Configuration* page > Web Messaging.

The following ''immediate status'' texts must be translated. Exchange the English text with your translation. Keep the code (20, 30 etc.) unchanged.

20	Message accepted
30	Memory full in message service
31	Message deleted due to time-out
40	Message not sent, invalid Call ID
nst	Message not sent
nlc	Message cancelled, no license
sto	Status time-out from message service
sns	Can't receive status
nan	Message cancelled, no Call ID
oor	Call ID(s) out of number range
	Unknown returncode, confused!

Example GUI index4 (default NetPage User Interface)

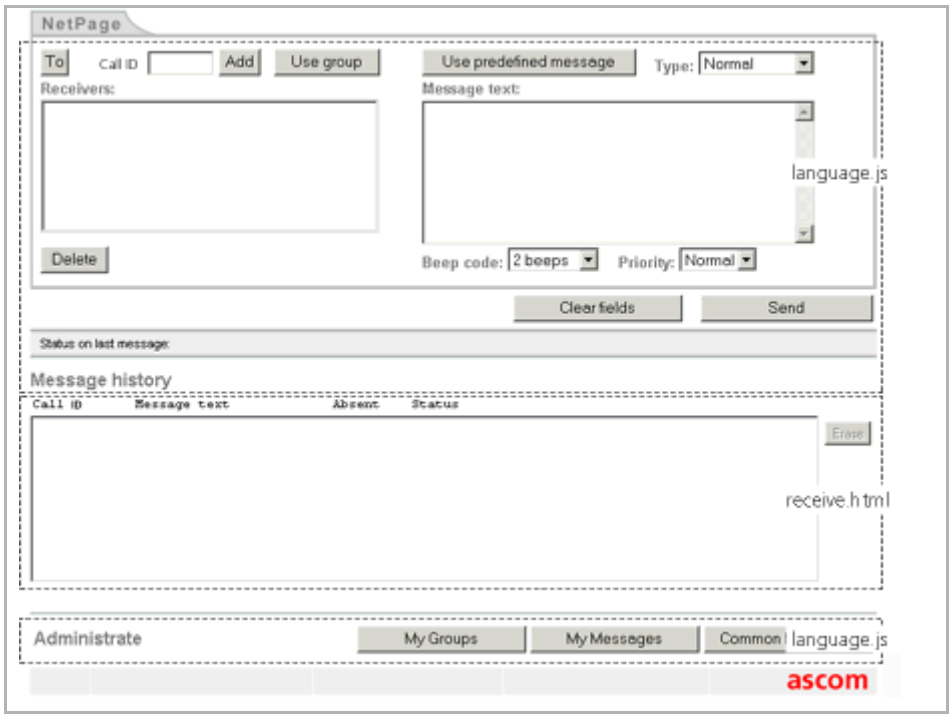


Figure 78. Files used for translation of the default user interface (index4).

Text which needs to be translated, is found in two different files. Translation of texts in the user interface (including text in Administrate pages, but excluding text in the Java Applet) are found in the ''language.js'' file. Translation of the Java Applet (Message history field) is found in the ''receive.html'' file, see figure 78 on page 177.

NOTE: The default NetPage GUI can be translated into language with UTF-8 character encoding.

1 Download/copy the files ''language.js'' and ''receive.html'' from the FTP area, see 22.2.2 Files for Translation/Editing on page 171.

2 Open the ''language.js'' file in a text editor, for example Wordpad. Add the translation inside the quotation marks after the English text, see example below:

''*Add Group*'', '' '' will become ''*Add Group*'', ''*Your translation*''.

Save the file.

3 Open the ''receive.html'' file in a text editor, for example Wordpad. Add the translation inside the quotation marks after the English text, see example below:

PARAM NAME=''English text'' VALUE=''Your translation''.

Save the file.

4 Upload/paste the files to the FTP area, see 22.2.7 Upload the Files to the FTP Area on Unite CM on page 178.

NOTE: The parameter ''Default GUI'' must be set to ''Custom''. The parameter is found on the *Advanced Configuration* page > Web Messaging.

5 Refresh the page and check the result. All buttons except the Administrate area buttons, will expand/decrease when the text is translated. The width of the Administration buttons is fixed but can be altered in the HTML file ''admin.html''.

22.2.7 Upload the Files to the FTP Area on Unite CM

Upload all updated files (including GIFs and CSS) to the FTP area.

1 Log on to Unite CM with an FTP client. Note that how to log on can differ between different FTP clients.[1]

Default username is ''ftpuser'' and default password is ''changemetoo''. xxx.xxx.xxx.xxx is the host name.

Examples:

- Windows Explorer: fill in ''ftp://username:password@xxx.xxx.xxx.xxx'' in the address field.
- Firefox: fill in ''ftp://xxx.xxx.xxx.xxx'' in the address field and log on with ''username'' and ''password''.

2 Upload the files to the *netpage* folder on the FTP area.

22.3 Test the New User Interface

It is recommended to test the customized user interface as follows, for example:

- If a company logotype is added, check that it looks all right and that Unite CM opens quickly. If Unite CM opens slowly, minimize the picture file size and save it as ''interlaced'' to decrease wait time for the image.

1.Internet Explorer is not an FTP client so its not possible to copy and move files from Internet Explorer.

- Check that all text is correctly translated.
- Send a message.
- Check that the ''message history status'' is received and displayed.

22.4 Update the User Interface after a new Unite CM Release

When a new version of Unite CM is released, there might be changes in the user interface that need to be translated.

1 Import your old translated file to the new Unite CM software version. New text and buttons in the user interface are shown in English.

2 Click the language file link and save it.

3 Open the file. All tags that are not translated are marked with the comment:
<!-- The text identifier below couldn't be translated -->

4 Translate the new text and import the translated file again.

23 System Supervision and Security

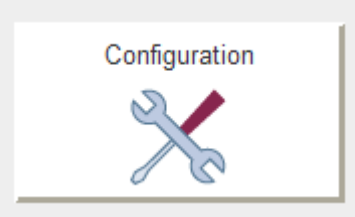


Figure 79. Configuration

23.1 Unite Modules

23.1.1 System Survey

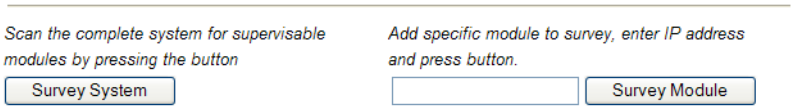
It is possible to survey other Unite modules in the system. All Unite modules connected to the LAN (System Survey) or just one single module.

1 Click ''Configuration'' on the start page.

2 Select Supervision > Unite Modules in the menu on the *Configuration* page

3 Click ''Survey System'' button located at the bottom of the Unite Module overview page to start a system survey.

- To survey one single module, enter the IP address for the module and then click the ''Survey Module'' button.


Scan the complete system for supervisable modules by pressing the button
Survey System
Add specific module to survey, enter IP address and press button.
Survey Module

When the system or a single module is surveyed, information about the module is shown. New modules that are found are shown in a separate list, New Modules. Modules that are lost since the last survey are shown in the list Lost Modules.

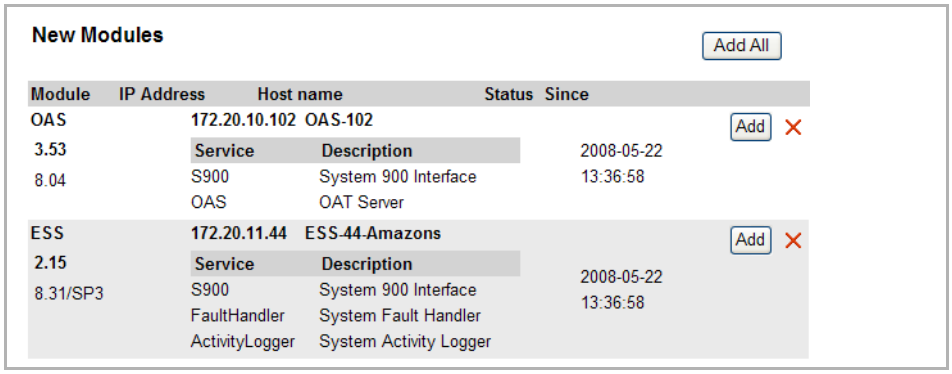


Figure 80. New surveyed modules

The survey request is sent out as a broadcast message, meaning that any module placed outside a router will not receive the request. If a module is placed outside the local LAN router, a specific request (Survey Module) to that module must be made for the first survey. Once the module has been added to the list of ''Existing modules'', it will be included in subsequent system survey requests. If an existing module is not answering on the broadcast message, a directly addressed survey request will always be sent.

4 Click the ''Add'' button to the right of the module in the New Modules list, see Figure 66, to add the module.

The added modules will be shown in the Existing Modules list.

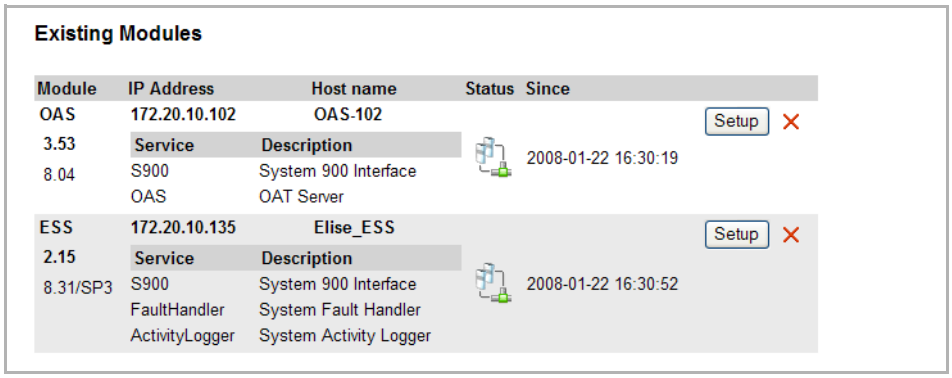


Figure 81. List of existing modules at a definite time

System Survey Status Symbols

When a system or module is surveyed, but not supervised, the status symbol for each module will show Module not supervised, see below.

Symbol	Description
	Module not supervised
	Module lost

Unite Module Overview

When all modules have been set up for survey, the Unite Module overview page gives a snapshot of the system at the time stated uppermost on the page.

If a new system survey is wanted, click the ''Survey System'' button again. If any new modules have been added to the system since the last survey, they will be shown in the ''New modules'' list and can be set up to be supervised.

Remove Unite Modules from the Overview

If a module is physically removed from the system and a new survey is made, the module is not automatically removed from the Unite Module overview page. The result of the survey for that module will be ''Module lost''.

To remove the module from the Unite Module overview page, click the ''Delete'' symbol. A dialogue window opens, click ''OK'' to remove the module.

23.1.2 System Supervision

Unite CM can supervise the modules that respond to a survey request. A request will be sent to the module with the specified interval, default set to 30 seconds. Unite CM can send a supervision request (either to a Unite module or an ICMP ping) every second, i.e. if the interval is set to 30 seconds up to 30 modules (Unite or IP Equipment) can be supervised. If this limit is exceeded, the interval will automatically be increased.

In the response, the module includes information about host name, software version, module key, license, start-up time and start-up cause. If the error relay is released, the response will include this information also which will result in the status ''Error'' in the overview.

Status Symbols	Description
	Supervision OK
	Module lost Appears in a ''Lost Modules'' list
	Module error
	Module not supervised

If the module does not answer on the request, Unite CM will generate a persistent Status Log. It includes the module type, IP address and host name of the non-responding module. The default level is ''Critical'', but can be changed on the setup page. It is also possible to add a customized text to the Status Log. The persistent fault will be cleared when Unite CM gets a response from the module.

When supervision is started/ended and when the supervision interval is changed, an Activity Log with information about the changes will be sent.

Change the Supervision Settings

On the Setup page, it is possible to choose if a module should be supervised or not and to set the interval (in seconds, default value is 30 seconds) at which Unite CM sends out a module status request to the supervised module. The fault level, event description and interface description can be edited from this page. There is also a direct link to the supervised module's Advanced Configuration page for basic configuration of the module.

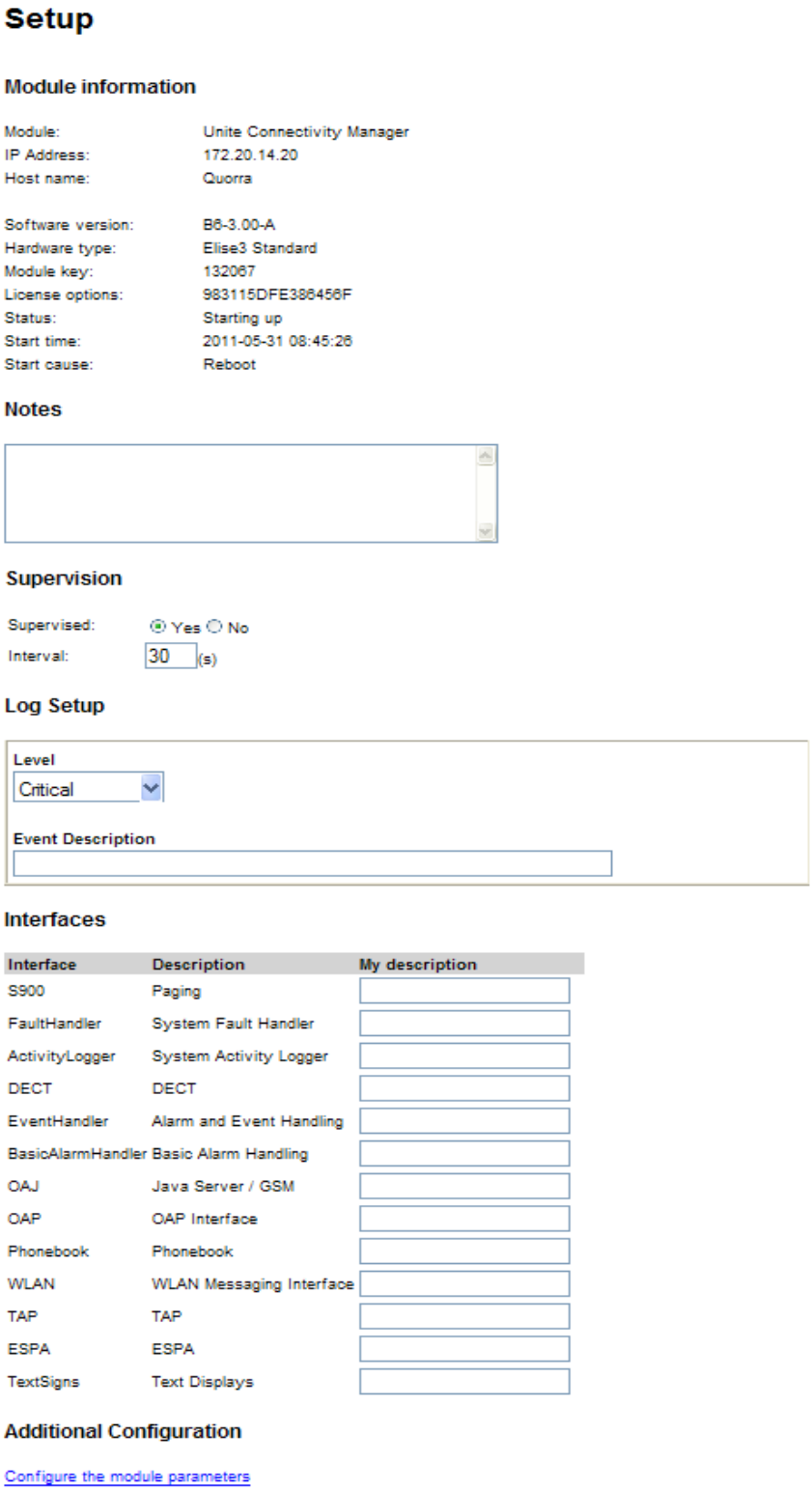
Note that changing settings is only possible for supervised modules in the *Existing Modules* list. Refer to 23.1.1 System Survey on page 180 for more information.

1 Click ''Configuration'' on the start page.

2 Select Supervision > Unite Modules in the menu on the *Configuration* page.

New modules in the system are found in a *New Modules* list and can be added to *Existing Modules* list by pressing ''Add''.

3 Click ''Setup'' for the module whose supervision settings should be changed.



4 Enter the following settings.

Settings	**Description**
Supervised:	If module/equipment should be supervised or not.
Interval:	The time between supervision request.
Level:	The fault level to use in the Status Log.

Event Description: A customized description that will be added to the Status Log.

Interface Description:
A customized description of the service.

5 Click ''Save''.

23.2 IP Equipment

Unite CM can supervise IP Equipment by sending ICMP ping requests. If the equipment does not answer on the sent request, a persistent Status Log will be generated. It includes the configured Equipment name and IP address or host name. The default level is ''Error'', but can be changed on the setup page. The persistent fault will be cleared when the equipment responds again.

Unite CM can send a supervision request (either to a Unite module or an ICMP ping) every second, i.e. if the interval is set to 30 seconds up to 30 modules (Unite or IP Equipment) can be supervised. If this limit is exceeded, the interval will automatically be increased.

Example: if the interval is set to 30 seconds as above, but the modules to supervise are 60, the interval will be increased to 60 seconds.

When supervision is started/ended and when the supervision interval is changed, an Activity Log with information about the changes will be sent.

1 Click ''Configuration'' on the start page.

2 Select Supervision > IP Equipment in the menu on the *Configuration* page.

Adding IP Equipment

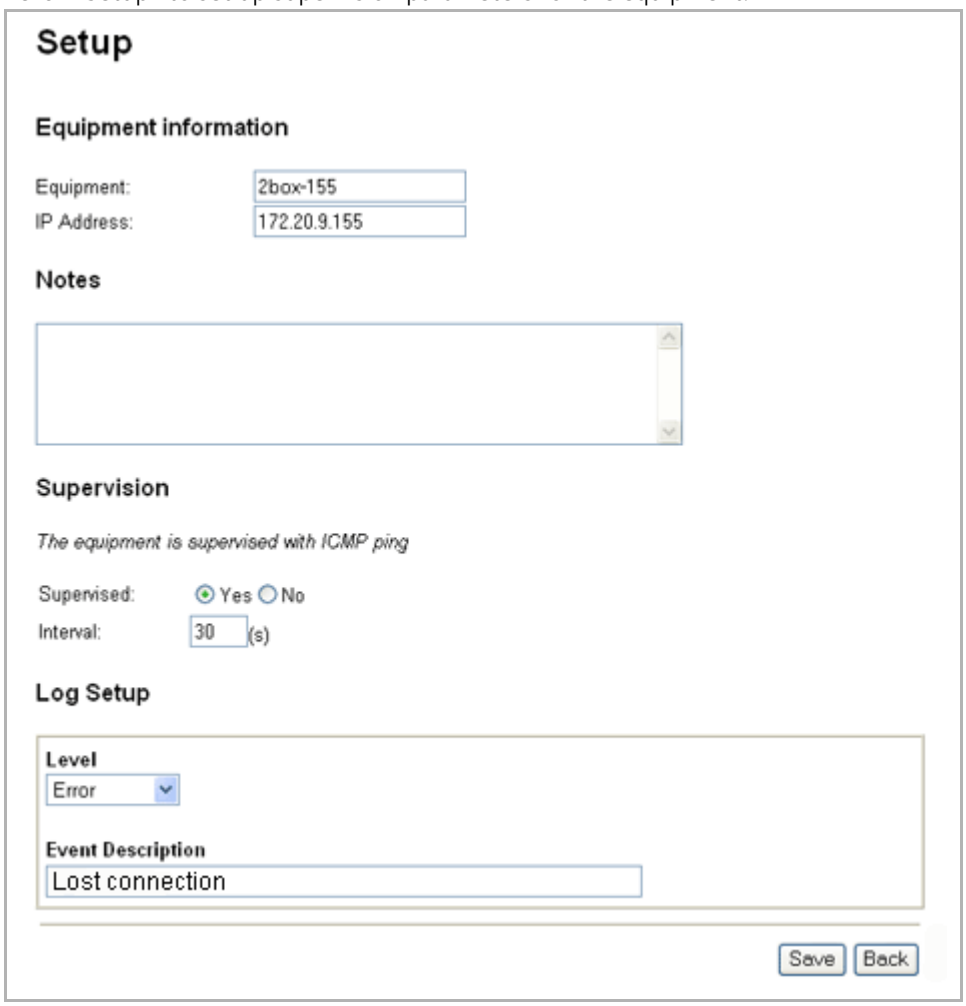
1 Enter IP address or host name.

2 Click ''Add IP Equipment'' to add equipment to the survey.

Status Symbols	Description
	Supervision OK
	Equipment lost
	Not Supervised

Changing Supervision Settings

1 Click ''Setup'' to set up supervision parameters for the equipment.



2 Enter a descriptive text in the Equipment field. Equipment is shown as Module in the Status Log.

3 Change IP address or host name if the address of the equipment has changed.

4 Select if the equipment should be supervised or not.

5 Enter the time between supervision requests.

6 Select fault level from the drop-down list to use in the transmitted Status Log.

7 Enter a description of the event and click ''Save''.

Removing IP Equipment

Remove IP equipment by clicking the ''Delete'' symbol. A dialogue window opens, click ''OK'' to remove the IP equipment.

23.3 Auxiliary Equipment

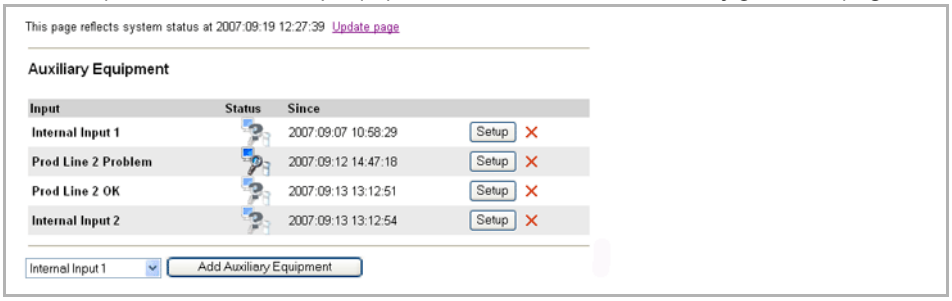
Unite CM can be configured to generate a Status Log when receiving an Input Activity. This can be used by equipment that indicates faults via a physical output to send faults to the Unite system. For each input that is monitored, equipment name, fault level and event description can be configured. It is also possible to set that the sent Status Log should be

persistent. The persistent fault will be cleared when the input is deactivated. The inputs are defined on the I/O Setup page.

When monitoring is started/ended, an Activity Log with information about the changes will be sent.

1 Click ''Configuration'' on the start page.

2 Select Supervision > Auxiliary Equipment in the menu on the *Configuration* page.



Adding Auxiliary Equipment

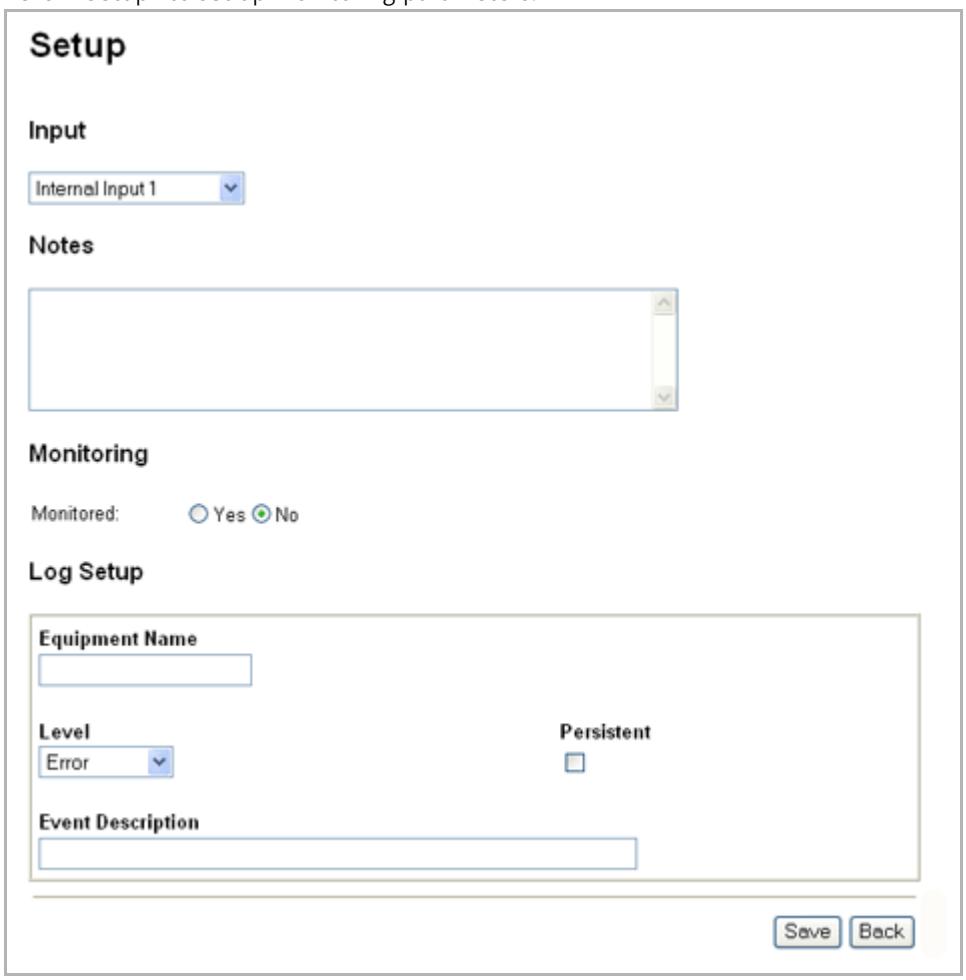
1 Select an Input from the drop-down list that contains all inputs configured on the I/O Setup page.

2 Click ''Add Auxiliary Equipment'' to add selected input.

Status Symbols	Description
	Monitored
	The input is not defined in the I/O setup.
	The auxiliary equipment has activated the input, i.e. signals a fault.
	Not monitored

Changing Monitoring Settings

1 Click ''Setup'' to set up monitoring parameters.



2 Enter/select following settings:

Setting	Description
Input:	The inputs are defined in the I/O setup page. The input can be changed, for example if the monitored equipment has been moved. Information about changes can be written in the Notes field.
Monitoring:	If the input should be monitored or not. When starting to monitor inputs from Unite CM, the status will always be OK regardless of the actual state of the input. This give that if the input is active when monitoring is started no Status Log is sent.
Equipment Name:	The name is shown as Module in the Status Log.
Level:	The level that the fault shall be reported as.
Persistent:	Select the Persistent check box, if a fault should remain until the input is not active any longer.
Event Description:I	Is shown under Description for the Status log.

3 Click ''Save''.

Removing Auxiliary Equipment

Remove auxiliary equipment by clicking the ''Delete'' symbol. A dialogue window opens, click ''OK'' to remove the auxiliary equipment.

23.4 SNMP Traps

SNMP (Simple Network Management Protocol) can be used by IP equipment to communicate that there are for example faults in the equipment.

Unite CM can be configured to generate a Status Log when receiving an SNMP Trap. The Status Log will include the IP address that the trap was sent from and text entered in the configuration. The information received in the trap can be added to the configured text.

The default action is to generate a Status Log with level ''Information'' for every received trap. The log level can be changed in the Log Setup.

It is possible to add SNMP Trap actions to get different behaviour depending on the sender's IP address and the information in the trap. The actions will be matched in the order displayed on the overview page and only one action will be executed.

By using wildcard *, several IP addresses can be matched in one action, for example ''172.20.*.*'' matches all IP addresses starting with 172.20. Wildcard* can also be used to match parts of the SNMP Trap message, for example ''Error*'' matches all messages starting with the word Error while ''*Error*'' matches all messages including the word Error.

Received traps can be discarded by selecting ''No Log'' in the Log Setup. This can be used either to discard traps from a specified address or with a specific message or in the default action to discard all traps that are of no interest (i.e. the ones that are not matched by the configured actions).

Information Received in Traps

The information in a trap is defined by the Management Information Base (MIB). It is defined by the equipment vendor and contains information about which traps the equipment can send. The received trap includes a hierarchically structured number called object identifier (OID) and optional variables.

For example, traps sent from Airespace equipment will have an OID starting with 1.3.1.6.4.1.14179, where 1.3.1.6.4.1 identifies that it is an enterprise specific trap and 14179 stands for Airespace.

When Unite CM receives a trap, it creates a string starting with the OID followed by a hyphen (-). Any received variables are added to the string after the hyphen. The filter set up in the SNMP trap action is matched against the created string.

Example:

When a Cisco access point restarts, a trap with OID 1.3.6.1.4.1.9.0.0 is sent. The first variable holds the uptime for the access point. Unite CM creates a string with the following appearance; 1.3.6.1.4.1.9.0.0-4 days, 21:56:52.90.

When setting up the SNMP trap actions, consult the MIB provided by the vendor for more information about the traps. In addition, set up the default action to include the received information in the sent Status Log and force the equipment to generate traps to get detailed information.

Default SNMP Trap Action

The default action will be matched for all traps that are not matched by any other actions that are set up. In the Status Log, the module will be set to ''-'' and the IP address and Event Description will be copied from the received trap.

1 Click ''Configuration'' on the start page.

2 Select Supervision > SNMP Traps in the menu on the *Configuration* page.

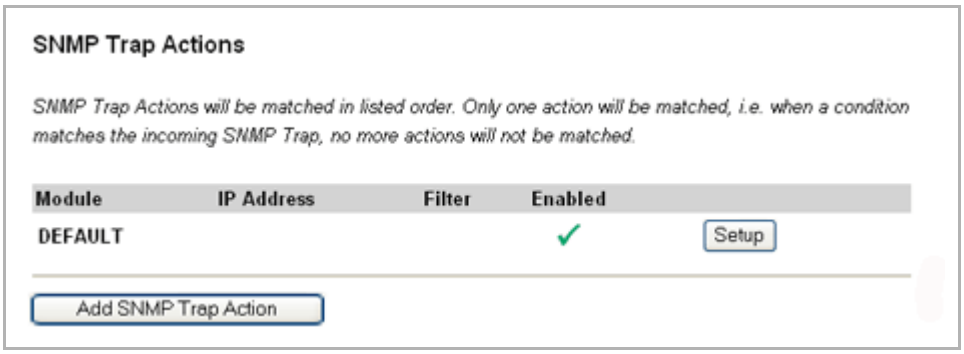

SNMP Trap Actions
SNMP Trap Actions will be matched in listed order. Only one action will be matched, i.e. when a condition matches the incoming SNMP Trap, no more actions will not be matched.
Module
IP Address
Filter
Enabled
DEFAULT
Setup
Add SNMP Trap Action

Figure 82. The default settings for SNMP traps action.

Change Status Level

1 Click ''Setup''.

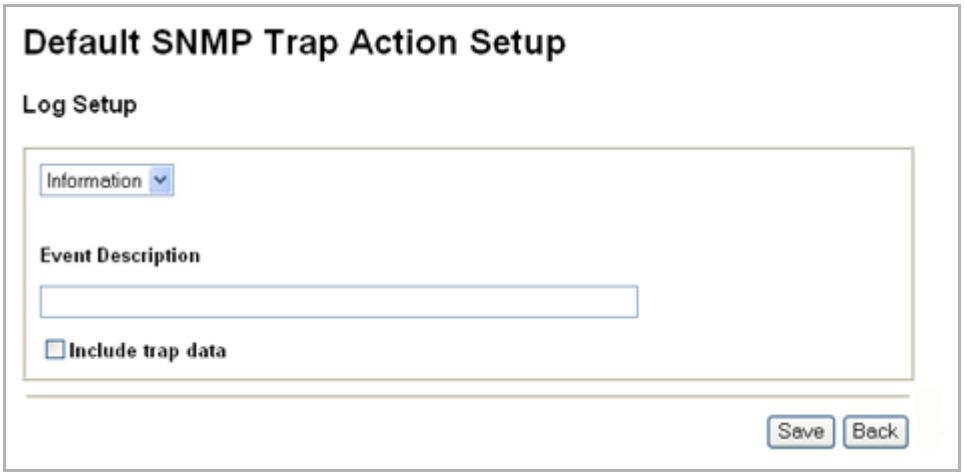


Figure 83. The default SNMP trap is enabled to receive information.

2 Select which level the sent Status Log should have or select ''No Log'' to not generate a Status Log when a trap only matching the default action.

3 Enter an event description to be included in the Status Log.

4 Select the Include trap data check box, if received trap data should be included in the log message and click ''Save''.

Add/Change SNMP Trap Action

This is used when SNMP traps from specific modules or with certain messages should be handled individually. The IP address in the received trap should match the defined pattern and/or the trap message should match the pattern set up in the filter. By selecting ''No Log'' in the Log Setup, traps matching the set up conditions can be discarded.

1 Click ''Add SNMP Trap Action''.

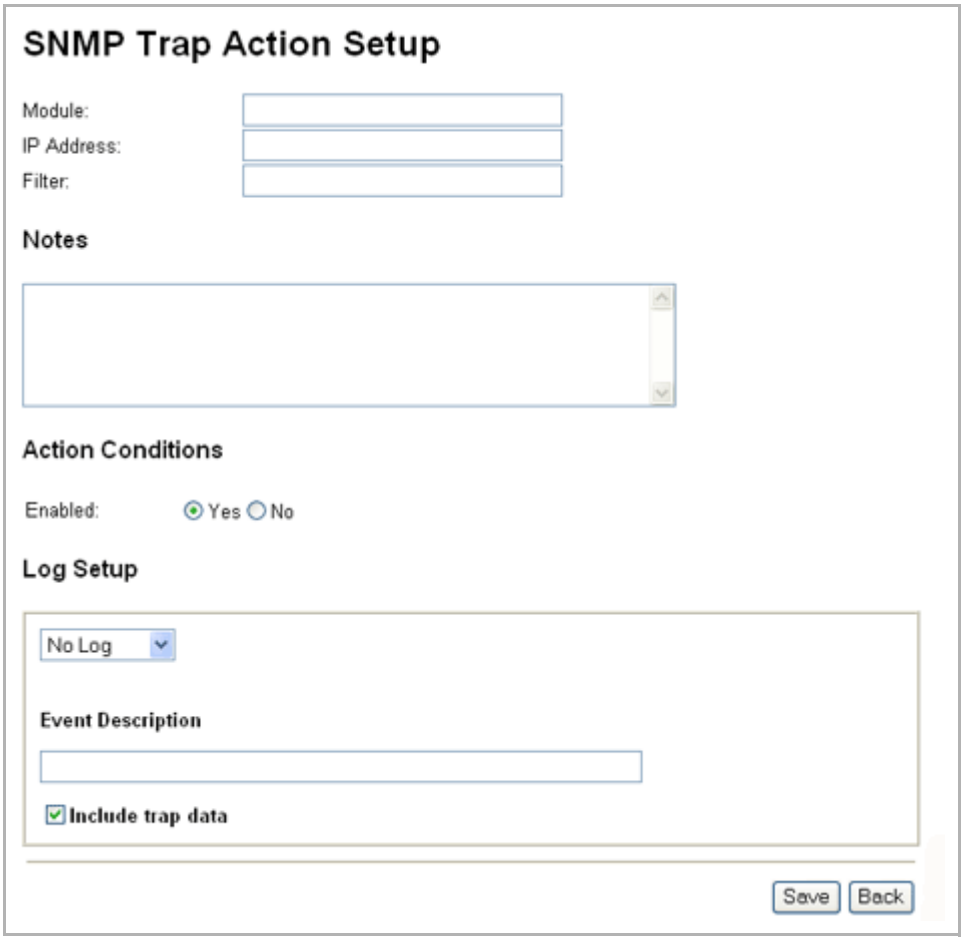


Figure 84. The action is setup to receive SNMP trap with the status Warning.

2 Enter/select following settings:

Setting	Description
Module:	Enter a name that describes the sender of the SNMP traps.
IP Address:	Enter the IP address pattern that should match the IP address in the received trap.
Filter:	Enter a text that should match the trap message. Wildcard (*) can be used to match a part of the received message. Leave the field empty if the trap should be received regardless of the trap message.
Enabled:	Select if the action should be enabled or not. If enabled, incoming SNMP traps will be matched with the IP address and the filter condition that is set.
Level:	Select which level the sent Status Log should have or select ''No Log'' to not generate a Status Log when a trap matching the conditions is received.
Event Description:	Enter an event description to be included in the Status Log.
Include trap data:	Select the Include trap data check box, if received trap data should be included in the log message

3 Click ''Save''.

Removing SNMP Trap Action

Remove SNMP trap action by clicking the ''Delete'' symbol. A dialogue window opens, click ''OK'' to remove the SNMP trap action.

23.5 Fault Handling

The fault handling in Unite CM makes it possible to start actions on an incoming fault. Possible actions are output activity triggering, sending a message, sending a fault notification via SNMP Trap or via E-mail. The actions start depends on trigger conditions.

Note that if Unite CM is to take care of faults from external modules, these modules must be configured to send their status log messages to Unite CM.

Functions in fault handling:

- Trigger conditions and action settings on faults
- Summary fault action settings on persistent faults

23.5.1 Nomenclature

Fault action: A fault action consists of trigger conditions that leads to an action, such as sending a message to a handset in the system and/or activating an output. One fault action can consist of several triggers and lead to several actions.

Trigger: A set of conditions that is used to match specific fault messages.

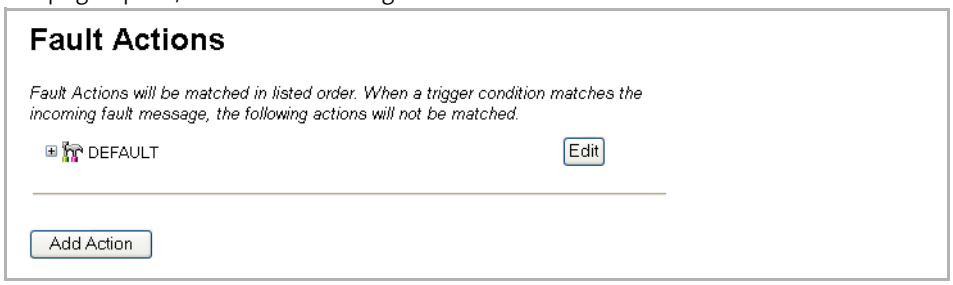
Action: Is started as a response to a trigger matching a fault message i.e. sending a message to a handset, activating an output or the error relay and sending SNMP Trap and E-mail.

23.5.2 Fault Actions

Settings of trigger conditions and actions are made in the Fault Actions page.

1 Click ''Configuration'' on the start page.

2 Select Fault Handling > Fault Actions in the menu on the *Configuration* page. When the page opens, a list of all existing actions is shown.


Fault Actions
Fault Actions will be matched in listed order. When a trigger condition matches the incoming fault message, the following actions will not be matched.
DEFAULT
Edit
Add Action

The action with the highest priority is shown first in the list, for example, at the top. The actions are processed in priority order. The Fault Handler only processes the first action that matches the incoming fault message, that is, only one action will be processed for each fault message. The priority order can be changed by using the arrows.

An action can be deleted by clicking the delete symbol.

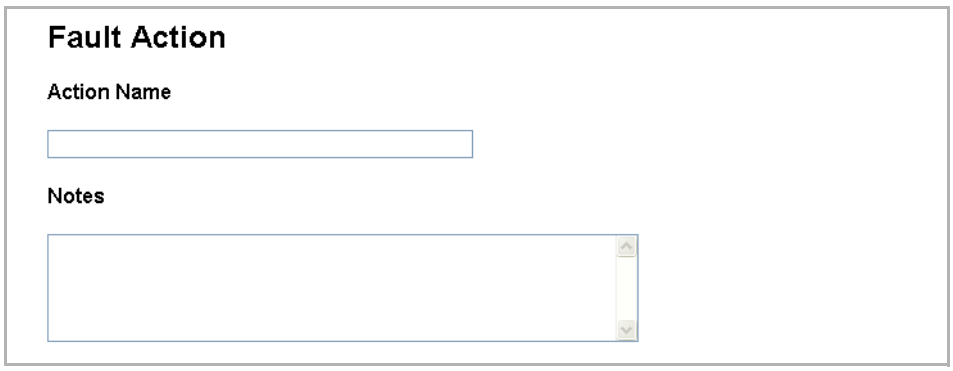
Default Action

The Default action is triggered on all faults that have not been processed by any of the previous actions. In the Default action, it is only possible to set actions since it is automatically triggered on all remaining faults. The Default action cannot be deleted and is automatically placed last in the action list.

Add Fault Action

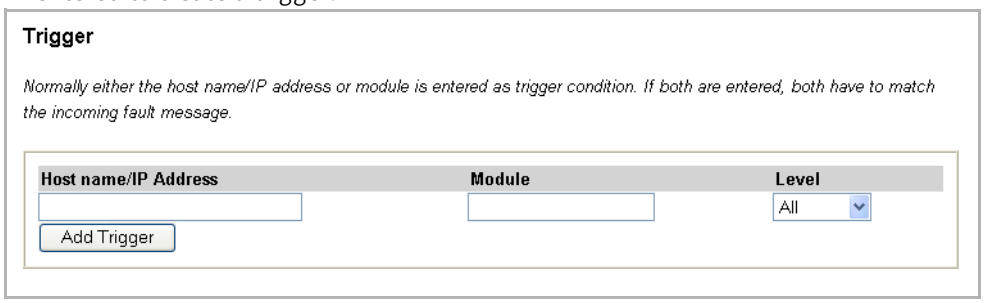
1 Click the ''Add Action'' button.

2 Enter the name of the action (mandatory) and additional text, if wanted, in the Notes field.



3 Enter the trigger conditions. The trigger can include either host name, IP address type of module or level of the fault. The type of module is found in the Unite Module overview page.

At least one of the three fields Hostname/IP address, Module or Level must be entered to create a trigger.


Trigger
Normally either the host name/IP address or module is entered as trigger condition. If both are entered, both have to match the incoming fault message.
Host name/IP Address
Module
Level
All
Add Trigger

4 The action can have more than one trigger. To add more triggers, click ''Add Trigger''.

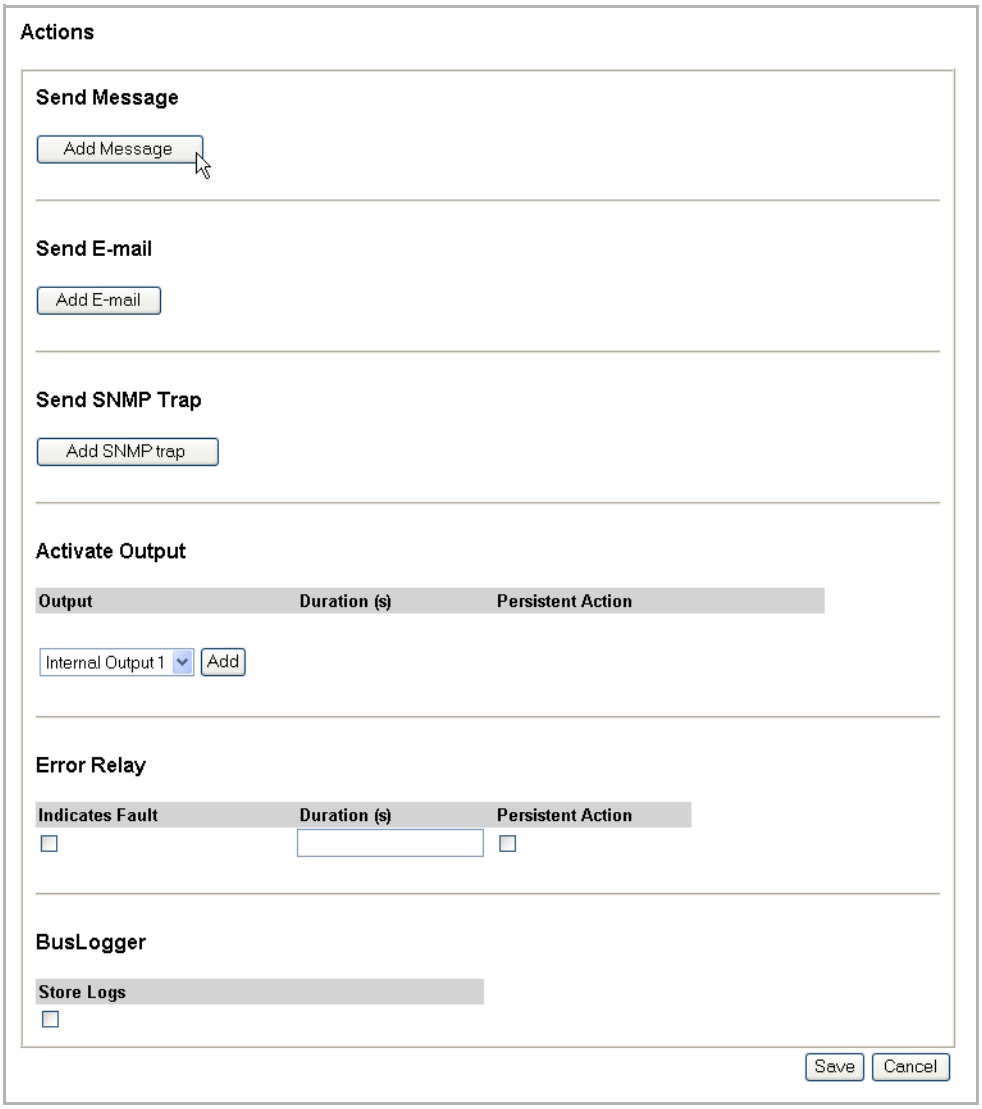
5 Define actions that indicate the fault, see descriptions under Define Actions below, how to configure the different types of actions.

6 Click ''Save'', located at the bottom of the page. The fault action is saved and added before the default action in the list on the Fault Actions page. By expanding the fault action, the triggers and actions are shown.

7 If needed, change the priority of the fault action by clicking the arrow symbols on the right side of the ''Edit'' button.

8 It is possible to edit a fault action by clicking the ''Edit'' button.

Define Actions



Message Action

1 Click ''Add message'' to define a message to send.

2 Enter the Call ID

NOTE: The Call ID must be defined as a messaging user in a Unite CM connected to your system. For example, if several Unite CMs are connected, the "local" Unite CM does not need to have the Call ID in its number plan. In this case, the local Unite CM must be connected to another Unite CM that holds the Call ID.

3 Enter the message text.

4 Select the "Include log info" check box to add the fault information to the message text.

5 Select the beep code level.

6 Select the priority level.

7 To add another message to send, click ''Add Message'' again.

E-mail Action

To be able to send E-mail from the Fault Handler, the IP address/host name of the mail server must be set up (defined in the Setup Wizard or 7.1 Mail Server Address on page 79).

1 Click ''Add Email'' to define an e-mail to send.

2 Enter e-mail addresses and any addresses that should receive a copy.

3 Enter a subject and a message text.

4 Select the Include log info check box to add the fault information to the message text.

5 Click "Save"

SNMP Trap Action

1 Click ''Add SNMP trap'' to define a SNMP trap to send.

2 Enter the IP address that the trap is to be sent to.

3 Enter the text that should be sent.

4 Select the Include log info check box to add the fault information to the message text.

5 Select SNMP version.

6 To send another SNMP trap, click ''Add SNMP trap'' again.

Output Action

1 Select the output to be activated and click ''Add''.

The outputs are configured on the I/O Setup page, see 4.8 Input/Output Setup on page 39. The state is set to the opposite of the inactive state when activated. For example, if output 2 is set to low in inactive state, the output will automatically be set to high when activated.

2 Set the duration in seconds. If the Persistent Action check box is selected, the Duration field can be left empty.
The output can be manually reset from the I/O setup page.

3 Select the Persistent Action check box to activate the output as long as the persistent fault remains. If not selected, the output will be active for the set duration also for persistent faults.

Error Relay Action

NOTE: When module redundancy is activated (see 4.14 Module Redundancy on page 65), the error relay should only be connected to the primary Unite CM since it is preferred to be the active module.

1 Select the Indicate Fault check box if the error relay should indicate faults.

2 Set the duration in seconds. If the Persistent Action check box is selected, the Duration field can be left empty.
The error relay will be released when activated. The error relay can be manually reset from the Active Faults page.

3 Select the Persistent Action check box to activate the relay as long as the persistent fault remains. If not selected, the relay will be active for the set duration also for persistent faults.

BusLogger Action

The Windows application BusLogger is used for error tracking in System 900 and Unite systems. An action in the Fault Handler can trigger the BusLogger to save current log information to disk, to prevent it from being overwritten.

Select the check box to make the BusLogger tool save current log information when the trigger is matched.

23.5.3 Summary Fault Actions

In the Summary Fault Actions page, it is possible to set actions to start when the first persistent fault occurs and/or when there are no remaining persistent faults. The actions that can be set are:

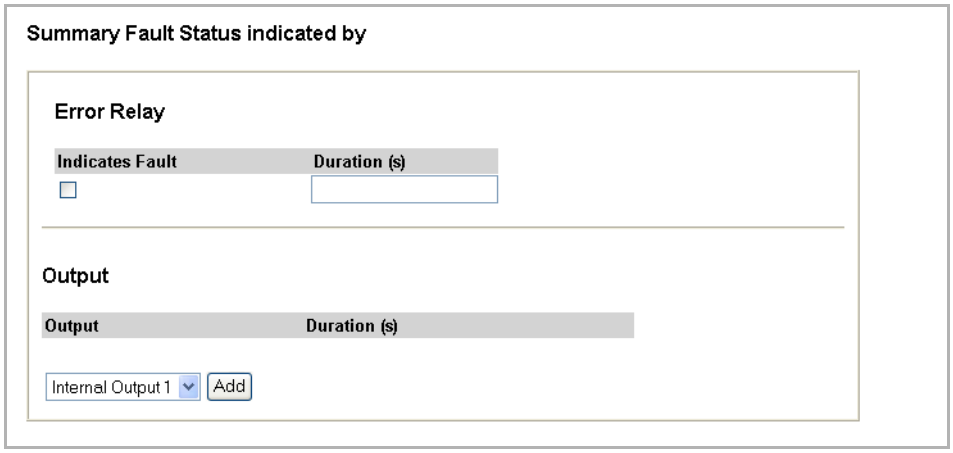
- Activating error relay and outputs set up on the I/O Setup page for the defined time or as long as there are persistent faults.
- Sending messages when the first fault occurs and when no faults remain.
- Sending SNMP traps when the first fault occurs and when no faults remain.
- Sending E-mail when the first fault occurs and when no faults remain.

1 Click "Configuration" on the start page.

2 Select Fault Handling > Summary Fault Actions in the menu on the *Configuration* page.

Activating Error Relay/Outputs

NOTE: When module redundancy is activated (see 4.14 Module Redundancy on page 65), the error relay should only be connected to the primary Unite CM since it is preferred to be the active module.



- Error Relay

1 To activate the error relay, select the check box for Indicates Fault.

The error relay will be released when activated.

2 Set the duration in seconds. If duration is not set, the error relay will be released until no persistent faults remain.

3 Click "Save" at the bottom of the page.

The error relay can manually be reset from the Active Faults page.

- Outputs

1 Select an output and click ‘‘Add’’.

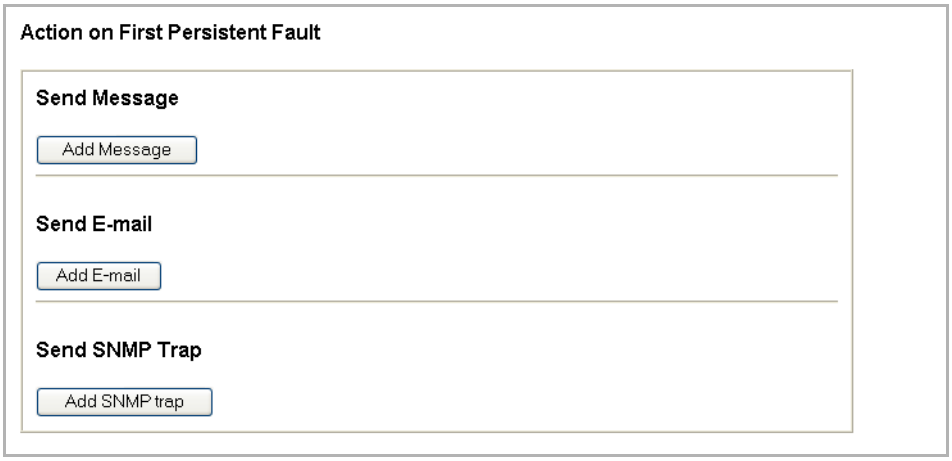
2 Set the duration in seconds. If the duration is not set, the output is active until no persistent faults remain.

3 Click ‘‘Save’’ at the bottom of the page.

The outputs can manually be reset from the I/O Setup page. See 4.8 Input/Output Setup on page 39.

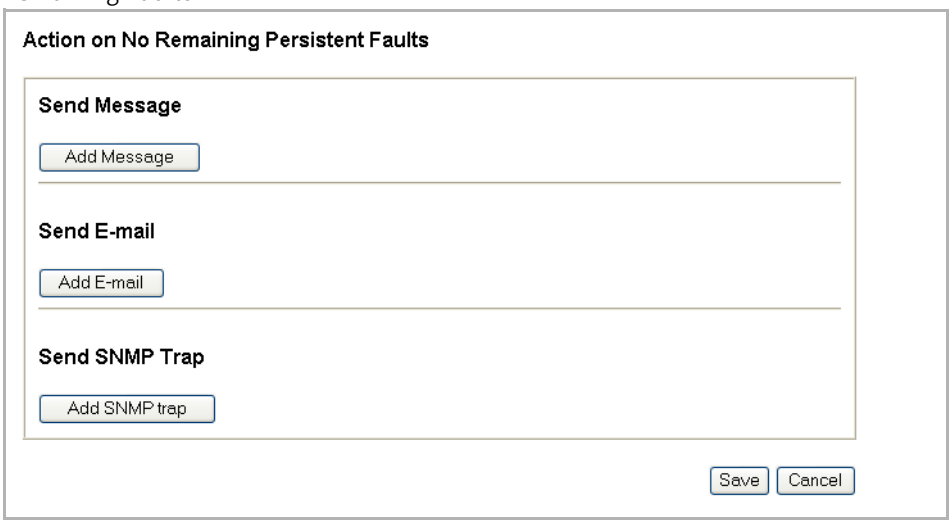
Sending Messages

- First Persistent Fault



  - Click ‘‘Add Message’’ in the Action on First Persistent Faults section to send a message for the first persistent fault. Refer to Message Action on page 193.
  - Click ‘‘Add E-mail’’ if an e-mail notification should be sent. Refer to E-mail Action on page 194.
  - Click ‘‘Add SNMP trap’’ to send a SNMP trap. Refer to SNMP Trap Action on page 194.

- No Remaining Faults



  - Click ''Add Message'' in the Action on No Remaining Persistent Faults section to send a message when all persistent faults are resolved. Refer to Message Action on page 193.
  - Click ''Add E-mail'' if an e-mail notification should be sent. Refer to E-mail Action on page 194.
  - Click ''Add SNMP trap'' to send a SNMP trap. Refer to SNMP Trap Action on page 194.

23.6 Activity Logging

To be able to view activities stored in Unite CM, it is also necessary to install the Java Runtime Environment to run the Activity Log Viewer. To find this, go to www.java.com.

Functions in the Activity Log:

- Activity Log Viewer – view and search for activities that are stored in Unite CM.
- Storage Settings – limit the number of stored activities.
- Log Export – automatic and manual export and clearing stored activities.

23.6.1 Activity Log Viewer

The Activity Log Viewer can be opened either from the start page or from the Configuration page.

1 Click ''Activity Log Viewer'' on the start page, or select Activity Log > Activity Log Viewer in the menu on the *Configuration* page.

2 Enter User name and Password and click ''OK''.

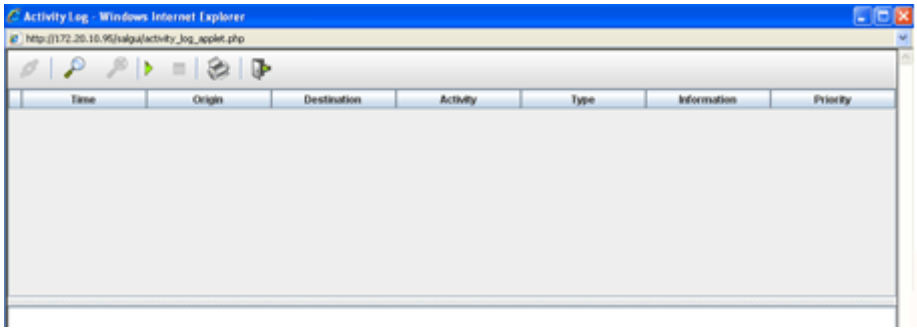


Figure 85. The Activity Log view.

It is possible to search for stored logs and view incoming activity logs continuously.

Symbols in Activity Log Viewer

Related activities

Search

Cancel Search

Update view continuously

Stop updating view

Print search result

Log out

Log information Symbols

 Error, did not reach destination.

Extended log, used for quick information and is not stored in database.

Search for Activity logs

From the Activity Log Viewer, it is possible to search for activities that are stored in Unite CM by choosing; time period, priority level, kind of activity etc. For priority and activity it is possible to specify if searching for all priorities or activities or searching for a specific priority or activity. Specific information in the activity can also be searched, for example a subject or body or a specific Call ID.

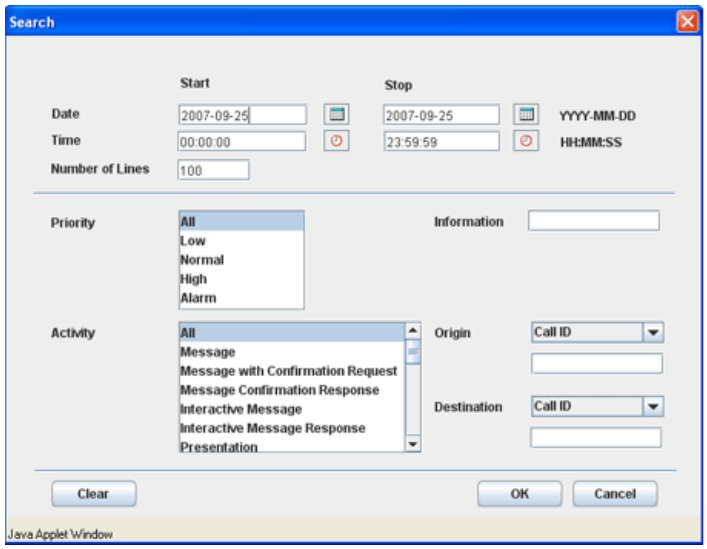
1 Click the search symbol.

2 Enter start date or click the ''calendar'' button to select the date. The time can be changed by clicking the ''clock'' button.

3 Change the number of lines if you want more or less than 100 activities to be displayed.

4 Select/specify the search criteria. All is set by default, but Priority, Activity, Origin, Destination and Information can be specified. When searching for specific Origin,

Destination and/or Information; enter number or a text in the corresponding text field.



Setting	Description
Date:	The date interval when the activities where logged. Default is the current date as both start and stop.
Time:	The time interval when the activities where logged. Default Start time: 00:00:00 Default Stop time: 23:59:59
Number of lines:	A numerical value between 1 and 1000. The default value is 100.
Priority:	The message priority; Low, Normal, High and Alarm. A combination can be selected by using ‘‘Shift’’ or ‘‘Ctrl’’.
Information:	A specific text in the activity log, for example a subject or body. Supported characters: Latin-1
Activity:	The different activities, for example Message or Input Activity. A combination can be selected by using ‘‘Shift’’ or ‘‘Ctrl’’.
Origin:	A specific origin such as; Call ID, User, Number/Address, IP Address.
Destination:	A specific destination such as; Call ID, User, Number/Address or IP Address.

5 Click ‘‘OK’’.

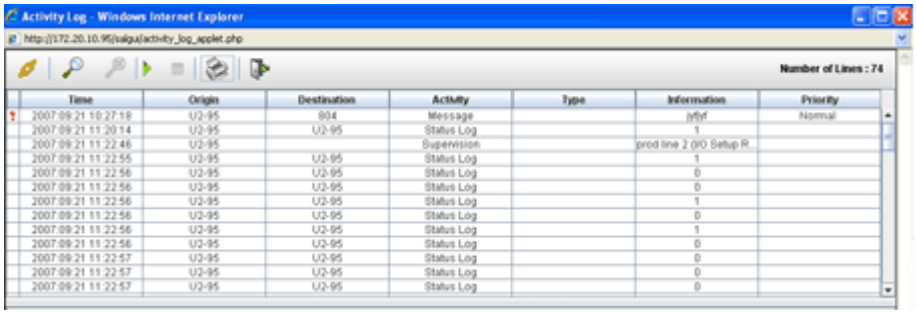


Figure 86. Search result of activity logs.

During the search, it is possible to interrupt the search operation by clicking the stop search symbol. An ongoing search is indicated with a symbol in the upper right corner. When the result of activities is displayed, the number of returned lines is displayed in the upper right corner. If more lines than displayed are available in the database, the information will be replaced with Number of Lines > X in red colour, where X is the number of requested lines.

When marking a log, more information about the log will be found below the list.

Print Search Result

The table with search result can be printed by clicking the ''printer'' symbol.

Details for a specific activity log can be printed by marking desired log, right-clicking and selecting ''Print Details'' from the displayed menu.

View Related Activities

To view related activities, for example all actions that have been taken as a result of an incoming alarm, click the activity log and then click the ''Related Activity'' symbol in the toolbar. (It is also possible to double-click the actual activity to open the related activity view or to right-click the activity log and choose Related Activities from the displayed menu.

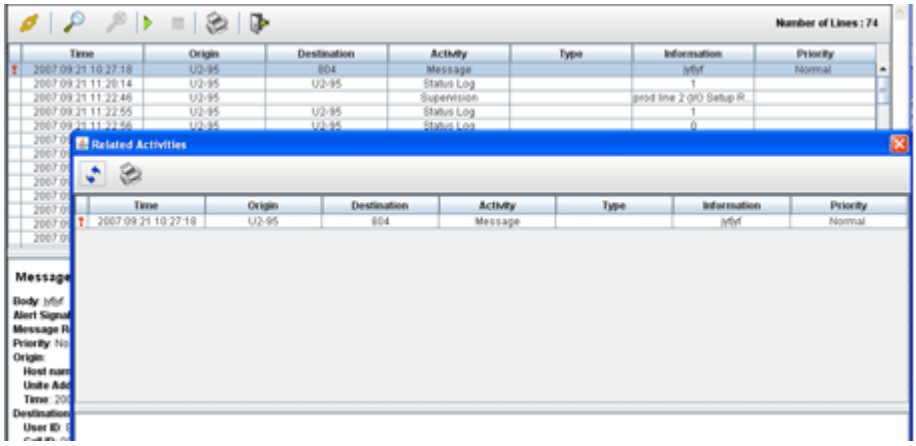


Figure 87. Related activity view.

Print Related Activities

The table with the related activities can be printed by clicking the ''printer'' symbol.

Details for a specific activity log can be printed by marking the log, right-click and selecting Print Details from the displayed menu.

Continues Log View

By clicking the ''Update view continuously'' symbol, the activity logs will be displayed when received by Unite CM. The logging can be stopped by clicking the ''Stop updating view'' symbol. It is also possible to pause by selecting the ''Lock scrolling'' check box.

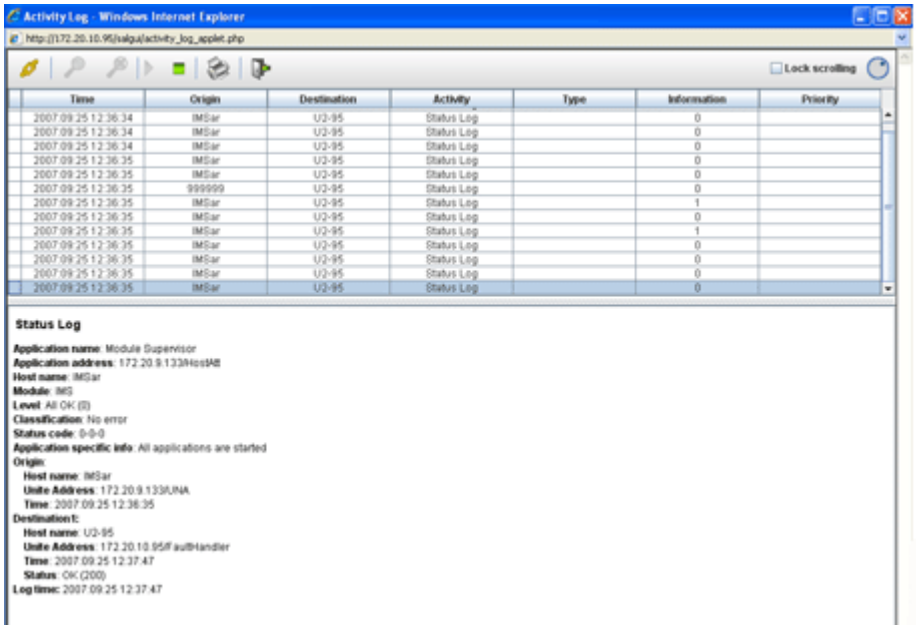


Figure 88. The information of the most recent activity logs are viewed.

The symbol located next to the ''Lock scrolling'' check box, indicates that the continuous view is activated.

When the extended activity log is enabled for a module, the symbol for extended activity logs will show up in front of incoming intermediate logs. This log is only for quick information, a ''real'' activity log will appear shortly after.

23.6.2 Storage Settings

Figure 89. The Storage Settings page, showing the basic storage settings.

The storage settings are divided into basic settings and advanced settings. With the basic settings, it is possible to store activities based on set priority. This concerns messages,

messages with confirmation, interactive messages and responses on messages, all other types of activities will be stored. In the advanced settings, it is possible to configure whether or not to store depending on receiver/sender and type of activity.

Basic Filter Settings

All check boxes for priority are selected as default, which means that all messages will be stored. The different priorities are:

- Low
- Normal
- High
- Alarm

NOTE: Alarm refers to the message priority Alarm.

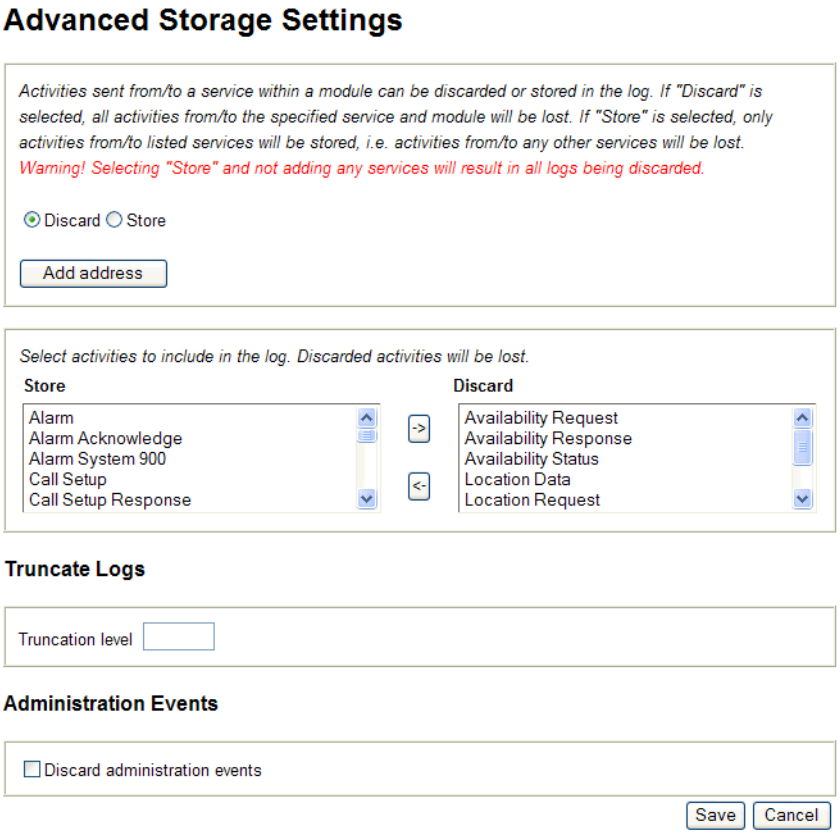
- Discard Messages with specified Priority

1 Clear the check boxes for message priorities that are not to be stored.

2 Click ''Save''.

Advanced Filter Settings

Click ''Advanced Settings'' to open the page. It is possible to discard or to store activities sent from/to an IP address and a service. It is also possible to select specific activities to be discarded regardless of sender/receiver.


Advanced Storage Settings
Activities sent from/to a service within a module can be discarded or stored in the log. If "Discard" is selected, all activities from/to the specified service and module will be lost. If "Store" is selected, only activities from/to listed services will be stored, i.e. activities from/to any other services will be lost.
Warning! Selecting "Store" and not adding any services will result in all logs being discarded.
Discard Store
Add address
Select activities to include in the log. Discarded activities will be lost.
Store
Alarm
Alarm Acknowledge
Alarm System 900
Call Setup
Call Setup Response
->
<-
Discard
Availability Request
Availability Response
Availability Status
Location Data
Location Request
Truncate Logs
Truncation level
Administration Events
Discard administration events
Save
Cancel

Settings	Description
Discard (default):	All activity logs will be stored if nothing else is specified. If Discard is selected and IP Address/Service is specified - Note that all activities from/to the specified service or module will not be stored.
Store:	Only activities from/to listed IP addresses/services will be stored. Note that all activities sent from another address/service than specified will be lost.
IP Address/Service:	On the format: xxx.xxx.xxx.xxx/service
Truncation level:	Specifies number of message characters to store in the database before truncation. 1 - 100 characters can be entered. If left empty the default characters level will be used, 100 for subject and 200 for body.
Discard administration events:	Specifies if administrational events shall be filtered out or not.

3 Click ''Save''.

- Discarding Activities based on Type

It is possible to discard activities regardless of the sender/receiver. By default, the following activity types are discarded; Availability Status, Location Data, Presentation and Presentation Response.

1 Select activities from the Store box that should not be included in the log.

2 Move the activities into the Discard box with the arrow button.

3 Click ''Save''.

23.6.3 Log Export Settings

Stored activities can be exported, either manually or automatically in CSV or XML file format. Automatic export can be to send logs to an FTP server or attach logs to an e-mail.

Manual export is used when a certain time period of the activity log should be exported and automatic export is used when the activity log should be exported regularly, for example the same time every day. On this page, it is also possible to clear all stored Activity Logs.

1 Click ''Configuration'' on the start page.

2 Select Activity Log > Log Export in the menu on the *Configuration* page.

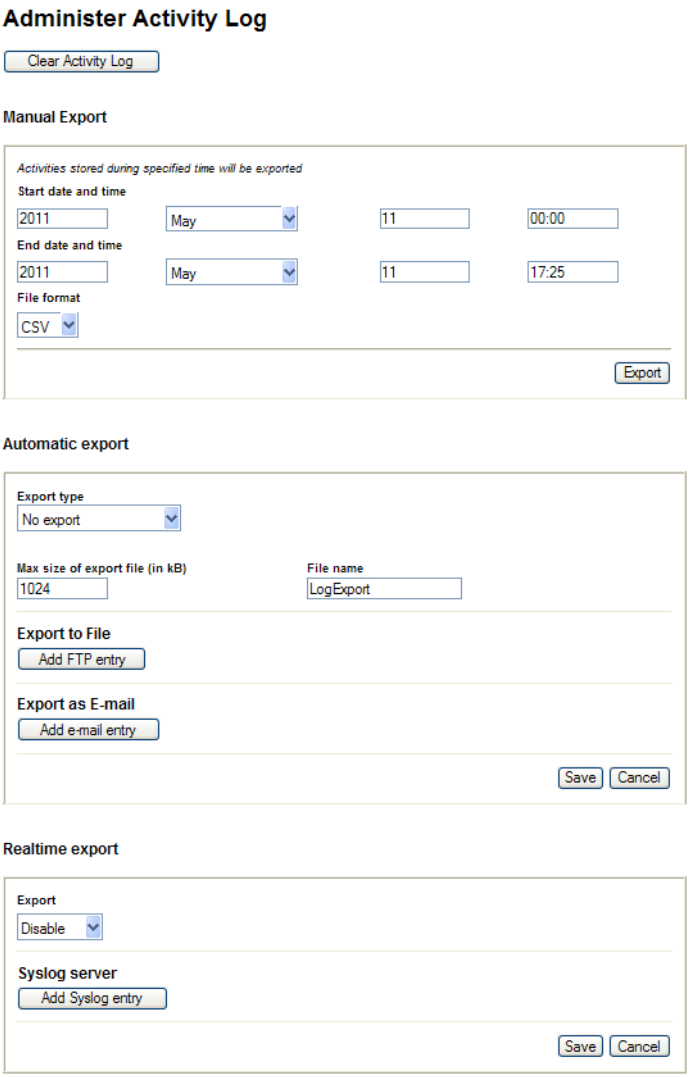
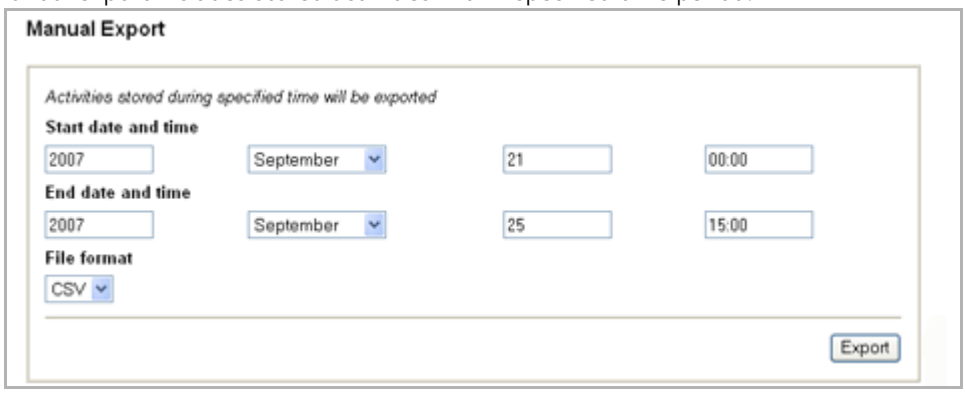


Figure 90. Administrate Activity Log page.

Manual export

The manual export includes stored activities within specified time period.



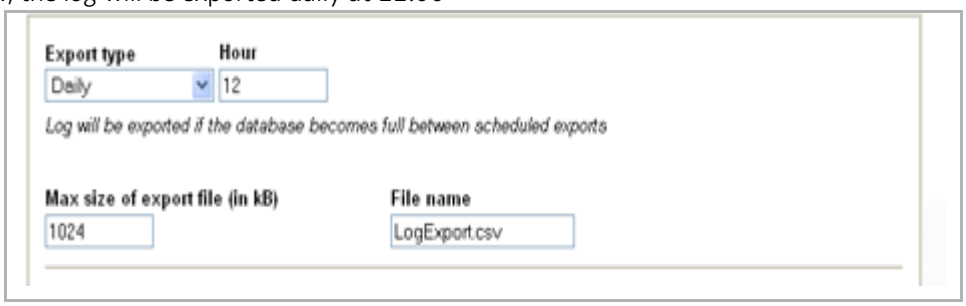
1 Enter/select the following settings:

Settings	Description
Start date and time:	For example, 2005, June, 04, 14.30
End date and time:	For example, 2005, June, 05, 02.00
File format:	Export in the format CSV or XML. If the log file should be analysed with the Log Analyser, then XML format should be chosen. Otherwise the choice of format is dependent of the tool that should be used for analysing the data.

2 Click ''Export''. A dialogue window will open where the activity log can be saved to the local file system.

Automatic export

The automatic export can be done regularly or when the database is full. If the exported data exceeds maximum file size, the data will be divided into several files. In the picture below, the log will be exported daily at 12:00



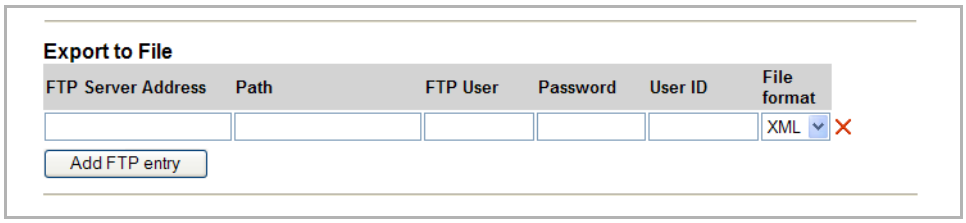
1 Enter/select the following settings:

Settings	Description
Export type:	Predefined values to choose from, for example; No export, Database full only, Daily, Hourly etc. Depending on the chosen value, the page will look different. Enter time data in the fields, if the chosen export type is time based.
File size:	100 - 30 000 kB. Enter max. size in kB of exported file. If file becomes larger, exported data will be divided into multiple files or e-mails.
File name:	File name to use when exporting the activity log. A time-stamp and a counter is added after the file name for each new file that is exported.

2 Define if the automatic export should be sent to a file or as an E-mail, see separate descriptions below how to configure the different types of exports.

- Export to File

1 Click ''Add FTP entry''.



2 Enter/select following settings:

Settings	Description
FTP Server Address:	IP address for the FTP server.
Path:	The path to a directory on the FTP server where exported files should be placed.
FTP User:	User name to log in to the FTP server.
Password:	Password for entered user.
User ID:	Enter ID if only the activities the user is allowed to see shall be exported. If left empty, all activities will be exported.
File format:	Export in the format CSV or XML. If the log file should be analysed with the Log Analyser, then XML format should be chosen. Otherwise the choice of format is dependent of the tool that should be used for analysing the data.

3 Click ''Save''.

- Export to E-mail

To be able to export via E-mail, the IP address/host name of the mail server must be set up (defined in the Setup Wizard).

1 Click ''Add E-mail entry''.

2 Enter/select following settings:

Settings	Description
E-mail Address:	Destination address for the export.
User ID:	Enter ID if only the activities the user is allowed to see shall be exported. If left empty, all activities will be exported.
File format:	Export in the format CSV or XML. If the log file should be analysed with the Log Analyser, then XML format should be chosen. Otherwise the choice of format is dependent of the tool that should be used for analysing the data.

3 Click ''Save''.

Export Activity Logs in Realtime to a Syslog Server

Activities in the module are logged and can be exported to a Syslog Server where the logs can be managed and analyzed. Messages are sent to the syslog server every time an activity occur in the module. Example of activities are: An SMS has been sent to a handset, an alarm has been received from a handset, an error has occurred in the module etc. Syslog is a simple protocol (SYStem LOG protocol) for transmitting event messages and alerts text across an IP network. The activities are sent as text messages from the module to the Syslog Server. The IP address to the Syslog Server must be set in the module. The activities can be exported to 5 syslog servers in parallel.

1 Select ''Enable'' in the drop-down list.

2 Click the ''Add Syslog entry'' button.

3 Enter the Syslog Server's IP address in the text field.

4 Click ''Save''

24 Troubleshooting

24.1 General Troubleshooting

Log files

When troubleshooting it is always a good idea to examine the log files, since they provide additional information that may prove useful. The first log to examine is the Status log, found under Status on the Configuration page, but when reporting an error to your supplier more advanced logs might be needed. Always include the appropriate log file. To find Info log and Error log:

1 Click ''Configuration'' on the start page.

2 Select Other > Advanced Configuration in the menu on the *Configuration* page.

3 Click the ''Troubleshoot'' button on the *Advanced Configuration* page.

4 Click ''View Info Log'' or ''View Error Log''.

Unite CM GUI does not start

To use the GUI, the computer must conform to the requirements listed in Data Sheet, Unite Connectivity Manager, TD 92739EN. If you do not have the correct software versions installed, contact your system administrator.

Firewall issues or no indication of connected device

If there is a firewall between Unite CM and any devices, the firewall may need some configuration to allow communication. See Appendix A for a description of used ports.

24.2 Device Manager Troubleshooting

Device does not show up in Device Manager

If a connected device does not show up as connected in the Devices view, check the status of the interface. Starting up mode is indicated during start of applications. If an application has lost connection to a required resource it is indicated as application problem mode. An Application problem is always shown as a persistent fault in the Status log.

If the information on the Configuration page shows Normal mode, it is not necessary to check the System information.

1 Click ''Configuration'' on the start page.

2 Select Other > Advanced Configuration on the *Configuration* page.

3 Click the ''Troubleshoot'' button on the *Advanced Configuration* page.

4 Select ''System information'' in the menu. The System Information page opens. Check system status.

Software in Device not recognised/synchronization fails

1 In the Devices view, check the parameter version for the device.

2 If the parameter version is highlighted with red, a package file (.pkg) including the software file and definition file with that parameter version must be imported to Unite CM. How to import a package file is described in the *User Manual, Device Manager in Unite Connectivity Manager, TD 92855EN*.

Software download fails

Possible causes:

- Portable is out of range, turned off or is not connected to the system.
- The LAN is badly configured and loses packages.
- The LAN is overloaded and loses packages.
- The web server containing the image file is overloaded.
- Erroneous image file.
- Erroneous path to the image file.
- The web server containing the image file is incompatible with the portable.

24.3 E-mail Interface Troubleshooting

If the SMTP E-mail interface does not work, it is recommended to check the following:

Check the Log Files

1 Open the Administration web page at http://xxx.xxx.xxx/admin and enter the user ID ''sysadmin'' and the correct password (default value is ''setmeup'').

2 On the ''System setup'' page, click on the ''Troubleshoot'' button and then select ''System Information''.

3 Scroll down to ''E-mail Interface'' and mark the check boxes ''Extended debug'' and ''Mail'', then click Activate.

4 Send an e-mail to Unite CM

View the log files

5 On the Unite CM Administration web page click the ''Troubleshoot'' button and then select ''View Complete Log''.

Send a Test E-mail via Telnet

1 Click on ''Start'' on the Windows task bar. Choose ''Run'' from the Start menu and write ''telnet'' together with the IP address of Unite CM in the field, followed by a space and ''25'' (port where Unite CM encodes SMTP).

2 Enter the highlighted text according to Figure 77.

```
telnet XXX.XXX.XXX 25
Trying XXX.XXX.XXX..
Connected to XXX.XXX.XXX
Escape character is '^]'.
220 Hostname ESMTP Ex in 19 May 2011 17:04:28
HELO localhost
250 Hostname Hello localhost [172.20.X.XXX]
MAIL FROM: user@domain
250 OK
RCPT TO: 123@domain
250 Accepted
DATA
354 Enter mail, end with "." on a line by itself
Subject: Hello

Body: Texttexttext
.
250 OK id=XXXXXX-XXXXXX-XX
QUIT
221 Hostname closing connection
```

Figure 91. Troubleshooting via Telnet.

A message is now sent to the call number 123. If the message reaches the Pocket Unit, search the fault outside Unite CM.

Check Mail Client Rules

For example, in Microsoft Outlook, select ''Tools'' and ''Rules wizard''. Also check that they are enabled.

Check that e-mails are redirected

The original sender name is shown only at a redirection, not a forward. E-mails must be redirected to ensure proper handling of manual acknowledge or user response data, else the e-mail reply will not reach the original sender.

Check that the DNS (domain name server) is stated

An mx-record for the Unite CM host has to be set up in the DNS, for example unitecm.company.com

Check that the Messaging System is not overloaded

If it takes too long for an e-mail to reach the recipient, or if e-mails do not reach the recipient at all because the message queue is full, then the Messaging system might be overloaded. This overload is seen in the log files of the interface module, for example the IMS.

24.4 Troubleshooting Guide

This section lists a number of possible faults, probable causes and suggested actions.

24.4.1 Troubleshooting Guide for the Device Manager

Fault	Probable cause	Action or comment
• The system does not have the correct time.	– Configuration error, no time server configured.	Configure the system to connect to a time server.
	– The time server is configured but is offline.	Restore connection to time server.
	– The web browser is selected as time source but the time has not been set by the user.	Set the time via the advanced configuration.
• An advanced charger does not come online in the Device Manager in a system with ''Service discovery'' enabled.	– The charger parameters for Service Discovery are not set.	Use PDM to configure the Service Discovery domain in the charger to the same value that is set in Unite CM.
	– The service discovery parameter ''Domain Name'' is not unique in the IP network domain.	Use PDM to reconfigure the charger to another service discovery domain. Make sure that the Unite CM is configured to use the same value
	– The advanced charger and the Device Manager are located in two separate IP networks that prevents the service discovery request.	Use PDMPDM to disable service discovery in the advanced charger and to set the IP Address to the Unite CM.
• An advanced charger does not come online in Device Manager in a system with ''Service discovery'' disabled.	The charger is configured to connect to a Device Manager with a ''Domain ID'' that is not used.	Use PDM to disable service discovery in the advanced charger and to set the IP Address to the Device Manager.
• The charger logs out immediately after log in and does not come online again.	The charger is already saved in the Device Manager that the administrator wants it to use. The Advanced Charger parameter in the desired Device Manager is pointing to another Device Manager (service discovery or IP address) which causes the charger to logout and connect to another Device Manager after completed synchronisation.	– Before connecting the advanced charger to the LAN, make sure that if the advanced charger is saved in the desired Device Manager it has parameters that points to the correct Device Manager. – Delete the saved charger from the Device Manager before connecting the charger to the LAN.

Fault	Probable cause	Action or comment
• The charger logs out immediately after login and comes online again after a while just to logout again.	The charger exists in two Device Managers and is saved in both. The parameters for the charger in Device Manager 1 causes the charger to login to Device Manager 2. The parameter for the charger in Device Manager 2 causes the charger to login to Device Manager 1. The charger jumps back and forth between the Device Managers.	Delete the charger from the Device Manager where the charger should be. The charger now logs in after a short while. Save the charger again. Delete the charger from the other Device Manager.
• Some devices report device busy in the Device Manager when the user is trying to change device parameters.	The device is occupied with some action that the device cannot combine with parameter synchronisation.	No action needed. The Device Manager will synchronise the changes when possible.
• Not possible to start a software download for some specific device types.	The device type is included in a baseline and manual software download is therefore disabled.	– Disable the baseline feature. – Exclude the device type from the baseline.
• Software download is stuck in pending.	– The device is not online.	Software download will start when device gets online.
	– Multiple devices are currently being updated.	There is a limitation in the Device Manager on the number of simultaneous software downloads. All devices are placed in a queue and will be upgraded in time. No action needed. Download will start in time.
• File downloads retrying.	The device is currently unavailable (device out of range, network problem)	No action needed. The download will start when the device comes in range again.
• Software downloads rejected.	The device is already updated with a new software but not yet restarted on the new software. This is due to selected activation time in previous software update i.e. ''When idle in charger'' or ''After manual restart''.	Restart the device manually and restart the download.

Fault	Probable cause	Action or comment
• Software downloads are aborted.	Wrong file selected for download to devices (External web server).	– Make sure that the URL to the desired software is correct and retry. – Make sure that the file is intended for that device.
• Low software download performance to handset inserted in charger.	The charger is not connected to the Device Manager (not online in the Device Manager). The handset is online only via OTA.	Configure the advanced charger so that it connects and logs on to the correct Device Manager.
• Communication failure to device.	The device did not respond in an expected way. The reason could be temporary communication problems caused by coverage problems or network problems.	Repeat the action after a while to see if it is possible to communicate with the device.
• No connection available for the Device Manager GUI.	– Max number of Device Manager GUI's has been reached.	Close the other Device Manager GUI to open new. A maximum of ten Device Manager GUIs can be connected.
	– The Device Manager server side is restarted due to reconfiguration.	No Action, the server will be up within a few minutes.
	– The Device Manager is temporarily unavailable due to restore of database.	No Action, the server will be up soon.
	– The network is preventing the GUI from connecting to the server.	No action.
• All devices log out after restore of a backup.	The backup is older than the device ''online status report timeout.''	No action. All devices will re-login within ''online status report timeout.'' (See device handling).
• Software files cannot be deleted.	The files are included in a baseline.	Remove the files from the baseline configuration. Delete the files.
• The parameter version is displayed in bright red in the Device Manager GUI.	There are no compatible .pkg files imported to the system.	Import a .pkg file suitable for the device. The .pkg file is provided by the supplier.

Fault	Probable cause	Action or comment
• The parameter version is displayed in dark red in the Device Manager GUI.	The version of the imported .pkg files are not 100% compatible with the device.	Import a .pkg file suitable for the device. The .pkg file is provided by the supplier.
• The parameter version of the Number in the Numbers tab is higher than in the parameter version of the device in the Devices tab.	The device has been downgraded to a previous software version with lower parameter version.	No action needed. This is not an error. The parameter version will be the same after a software upgrade has been performed on device.
• No numbers are visible of the selected device type in the Number tab.	The search field is red. Current search returns no hit.	Alter search or use "show all" to reset search to default.
• ''Go to number'' is dimmed out for a device in the device view.	The selected device has no number associated to it.	– Assign a new number to the device. – Associate a new or existing number to the current device.
• The handset is not visible in the Number tab.	– The handset has no number associated.	Assign or associate a number to the device.
	– The device is offline and not saved as number.	Bring the device online. Save the number in order to make it possible to edit the number when it is offline.
• Number creation of desired device type is not possible.	The .pkg file for the desired device type is not imported to the Device Manager.	Import the .pkg file for the desired device type. The file is provided by the supplier.
• It is not possible to apply a template at creation of new number.	No compatible template for the desired device exists.	Create a new template or upgrade an existing template and retry.
• A handset logs out when placed in an advanced charger	The device manager configurations in the IPBS and the advanced charger are not the same.	Delete the saved instance of the advanced charger in the Device Manager. Use PDM to reconfigure the advanced charger so that it will log on to the correct device manager. Connect the advanced charger to the LAN.

Fault	Probable cause	Action or comment
• The handset does not log on to the device manager OTA.	– The Domain ID is not set correctly in the IPBS.	Reconfigure it to match the device manager Service Discovery parameter Domain ID.
	– The system does not support service discovery.	Erase the Domain ID in the IPBS and set the IP address to the device manager under Advanced Settings > Device Management.
• The WLAN handset does not log on to the device manager OTA.	– Both IMS/IP and Unite CM are used. An i62 WLAN handset logs on to the IMS/IP. The IMS/IP does not support i62 which mean that it cannot forward the correct handset login information to Unite CM.	
• When trying to manage the license for a device, the status is changed to ''server failure''.	The firewall has closed port number 443 for https communication.	Reconfigure the firewall to allow https communications via port 443.

24.4.2 Troubleshooting Guide for Unite CM

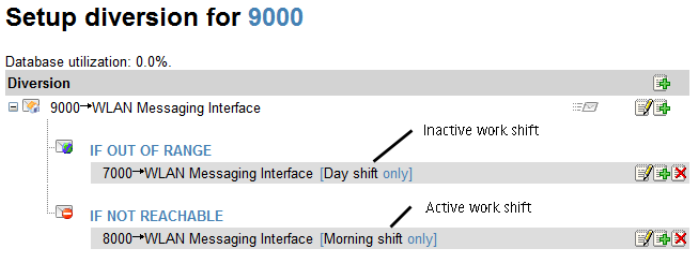
This part of the Troubleshooting Guide lists possible faults that are not connected to the Device Manager

Fault	Probable cause	Action or comment
• It is not possible to send SMS to a specific device.	– The device does not support SMS.	---
	– Unite CM license does not support SMS.	Upgrade the license to support SMS.
	– The IPBS UNITE SMS parameter is misconfigured.	Set the parameter so that it points out Unite CM containing the DECT Interface.
• It is not possible to edit the Central Phonebook.	– The phonebook is configured to be read-only.	Edit the external phonebook file and re-import it to the Central Phonebook.
	– The phonebook is configured to use an LDAP server	Access the LDAP server and alter the desired entry. After ''commit'', the new data will be available for the Central Phonebook.

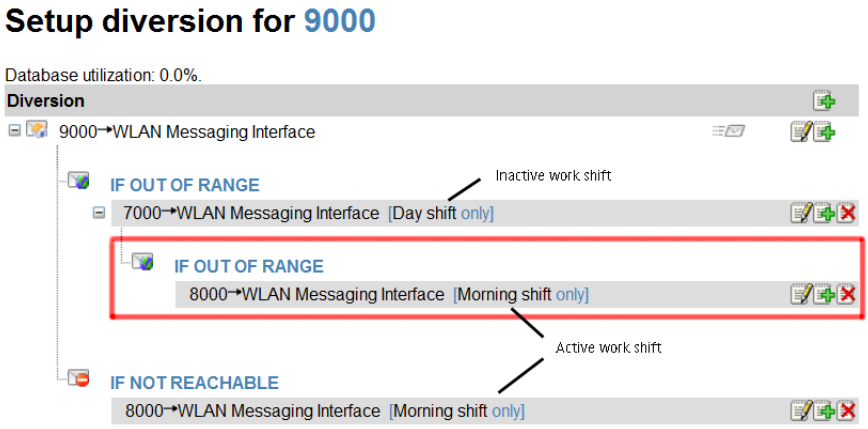
Fault	Probable cause	Action or comment
• LDAP queries sometimes returns no value.	– The phonebook uses Microsoft Active Directory which doesn't allow anonymously referrals.	Configure the phonebook to use port 3286 to Microsoft Global Catalog (GC) instead of port 389. GC is a service in Microsoft Active Directory. Configure GC to synchronize all attributes that is needed for users in the phonebook.
• Import of language to the configuration GUI fails.	The language file has the wrong format.	Export the default language to set the format and edit the language file.
• Set language fails in Unite CM.	– The language file might be faulty.	Try to import the language file again and verify that it is OK. If not, the file is corrupt.
• Several functions of the system does not start.	– There is not a valid license.	Enter a valid license and restart the module.
• Spontaneous restarts of the application Serial Interface is seen in the error log.	– Multiple applications.	Make sure you do not have multiple applications configured for Serial port 1, for instance GSM or DECT together with Serial Interface.
• Advanced diversion is not performed when diverting from an inactive work shift to an active work shift.	– This occurs when you have an Out of range condition in an inactive work shift, and a Not reachable condition in an active work shift. Since the Out of range condition not should be performed —due to it belongs to an inactive work shift — the Advanced Diversion function tries to use the Not reachable condition due to it belongs to an active work shift. In this case, the Not reachable condition will not be performed due to the Out of range condition blocks the Not reachable diversion.	See the example below for more information.

Fault	Probable cause	Action or comment

Example:



In the figure above, the Not reachable condition(8000->WLAN Messaging Interface) will not be performed due to the Out of range condition (7000->WLAN Messaging Interface) in the inactive shift blocks the Not reachable condition in the active shift.



The solution is to add an additional Out of range condition as shown in the figure above. In this case, the diversion will be sent to 8000 (if needed).

• A Call ID could not be found in the Number Plan when saving the Call ID in a Group ID, Fault Action Handler, or Basic Alarm Manager (BAM).	– You have entered a Call ID that is not defined as messaging user in the Unite CM.	Define a messaging user with the missing Call ID.
	– In a multi-site number plan, where several Unite CMs are used, has your Unite CM lost the connection to the Unite CM that holds the Call ID.	Add the Call ID by pressing "OK" in the dialog window that appears when pressing "Save". Check that your Unite CM has correct UNS Operating Mode settings. That is, your Unite CM must be connected to correct the Unite CM that holds the Call ID. .

24.4.3 Troubleshooting for NetPage

Fault	Probable cause	Action or comment
• My Groups and My Messages do not work.	– Cookies are not allowed in your web browser.	Check that cookies are enabled in your web browser.
• Number list or Common Messages are unsatisfactorily updated	---	Refresh the cache memory on the web browser. If they still are unsatisfactory, refresh catching proxy (if any). In, for example Microsoft Internet Explorer, this can be achieved by pressing CTRL+F5.
• Entire Message history including column headings doesn't appear	– The Java Virtual Machine may be missing on your computer.	Contact your IT department for assistance.
• Message history is not running, although messages are sent and column headings are visible.	– There might be a firewall preventing you from receiving data from the NetPage server.	Contact your IT department to open port number 5891 in the fire wall, in the direction from the web client to the NetPage server.
• Translation into language with character encoding UTF-8 is not displayed correctly in the NetPage's GUI.	– The software of Unite CM has been upgraded from an older software version to version 4.3x. The newer software has also inherit the older software's settings (for example by using the "Copy current settings" option).	Open the html files used by Netpage (located on the FTP area) in WordPad or similar text editor. Change the character encoding in the files to this: <meta http equiv= "Content-Type" content="text/html; charset=**utf-8**">

24.4.4 Troubleshooting Guide for Corridors Displays

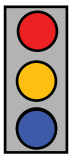
Fault	Probable cause	Action or comment
• The corridor display shows ‘‘No Data	The display has a proper connection to the network, but it has not been added to the text displays list.	Follow instructions in chapter 12.1 Text Display Settings on page 114.

24.5 LED Patterns and Troubleshooting Tools in Unite CM

Unite CM hardware has different LEDs to indicate the status and besides that the possibility to show active faults and logging the faults.

LED colors **Description**

The LEDs show different colors to determine type of information and have different flashing frequency for showing the priority



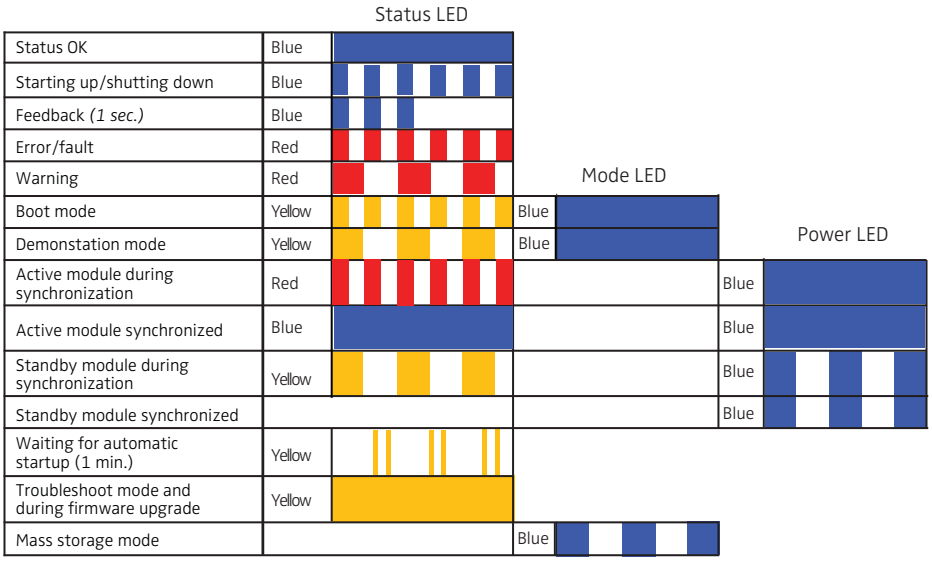
Colors

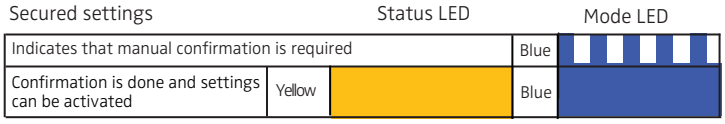
Red	Fault indication
Yellow	Mode indication
Blue	Normal operation (OK)

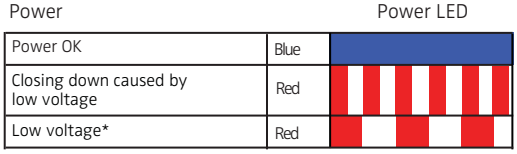
Flashing frequency

Fixed light	indicates normal state
Slow flashing light	indicates medium attention
Quick flashing light	indicates high attention

Flashing patterns







* also used if the Power parameter conflicts with the actual setup.

Demonstration Mode	Demonstration Mode is activated by pressing the Mode button for 10 seconds. Unite CM will then run with full functionality for 2 hours, then it returns to the configured license! If it works in Demonstration Mode and not in normal operation you probably have a license problem.
Active faults	Refer to 4.13.1 Active Faults on page 59.
Fault logging	Refer to 4.13.4 Fault Log on page 61 and 4.13.5 Administer Fault Log on page 62.
System Information	Refer to 23.1.2 System Supervision on page 182.
Site Information	Refer to 4.13.6 Site Information on page 63.

24.6 Advanced Troubleshooting

Unite CM Advanced Configuration page (requires system administrator rights) includes advanced troubleshooting. Snapshots of selected logs or a complete log can be viewed.

1 Click ''Configuration'' on the start page.

2 Select Other > Advanced Configuration in the menu on the *Configuration* page.

3 Click the ''Troubleshoot'' button on the *Advanced Configuration* page.

4 In the left menu on the Troubleshoot page you can view logs and find detailed information about the system.

- Specify Information to Log

Standard debug is set by default but this can be extended and show more details.

1 Click ''System Information'' in the left menu.

2 Enable desired logs and click ''Activate''.

- Send Test Message

The Troubleshoot page also includes the possibility to send test messages.

1 Click ''Send Test Message'' in the left menu.

2 Enter Call ID and click ''Send Message''.

24.7 What to consider when replacing a module

- IP Address
- License
- Module key
- Remember where cables were connected

24.8 Technical Support

For technical support please contact your local Ascom representative.

25 Related Documents

Data Sheet, Unite Connectivity Manager	TD 92739EN
Elise3 – Embedded Linux Server including safety instructions	M0275130
Installation Guide, Elise3	TD 92679GB
Data Sheet, Elise3	TD 92524GB
User Manual, Action Assignment in Unite Connectivity Manager	TD 92842EN
User Manual, Duty Assignment in Unite Connectivity Manager	TD 92841EN
User Manual, Device Manager in Unite Connectivity Manager	TD 92855EN
Function Description, Remote Management	TD 92257GB
Function Description, Open Access Protocol (OAP)	TD 92215GB
Function Description, Activity Logging in Unite	TD 92341GB
Function Description, System Supervision and Fault Handling in Unite	TD 92252GB
Function Description, Number Planning and Message Routing in Unite	TD 92254GB
Function Description, Product Licensing Overview	TD 92677GB
Function Description, Interactive Messaging (IM)	TD 92168GB
Installation and Operation Manual, Remote Management Client	TD 92256GB
Data Sheet, Alarm Modules T941AM8/AM32	TD 90862GB
Installation Guide, Alarm Module T941AM8	TD 90858GB
Installation Guide, Alarm Module T941AM32	TD 90854GB
Data Sheet, Output Module T941OM	TD 90964GB
Installation Guide, Output Module T941OM	TD 90859GB
Programming Guide, Event Handler	TD 92329GB
Programming Guide, Open Java Server (OJS)	TD 92230GB
Protocol, Serial Data Interface S942SI	TD 92088GB
System Description, Unite	TD 92243GB
System Planning, Unite	TD 92258GB

26 Document History

For details in the latest version, see change bars in the document.

Version	Date	Description
A	6 September 2010	First released version
B	30 September	Updates in chapter 1.1 and other minor changes.
C	7 June 2011	• Added chapters: 3.3.2 Set Password Policy on page 17 3.4 Disable the NetBIOS Service on page 18 3.5 Allow Fragmented TCP Packets on page 18 3.7 Message Routing Description on page 19 4.1.3 Import users from a CSV file on page 22 4.2 Additional User Settings on page 23 4.3 Create Groups on page 30 4.5 Create Work Shifts on page 34 4.11 Advanced Event Handling on page 51 7.1 Mail Server Address on page 79 7.2 UNS/User Server on page 79 7.3 Remote Service Center on page 81 8.6 CMG Parameter Setup on page 95 11 ASCII Interface on page 109 14 SMTP Mail Interface on page 120 22.2.5 Creating a URL Call on page 175 24.3 E-mail Interface Troubleshooting on page 209 B.4 Cables for Remote Management Client on page 230 Appendix G: ASCII-table on page 245 Appendix H: Extracting Information from HL7 v2 Messages on page 246. Appendix I: XML Message Handling in Event Handler on page 253. • Added Multiple Masters to chapter 15.1.4 IP-DECT on page 125. • Updated licence info in chapter 1.1 Licenses for Unite CM on page 1. • Removed Device Manager from this document. A new document ''User Manual, Device Manager in Unite Connectivity Manager, TD 92855EN'' has been created.
D	27 June 2011	Updates in chapter 1.1 Licenses for Unite CM on page 1 and 7.7 Java Server/GSM on page 85.
E	19 December 2011	Added chapters: 4.14 Module Redundancy on page 65 Appendix C: System 900 Connections on page 232 Appendix D Updated chapters: See change bars for additional changes.

Version	Date	Description
F	05 March 2012	Updated chapters: 7.2 UNS/User Server on page 79: Note added regarding ESS. 7.12 Setting License Number for Unite CM on page 89: clarification on how to enter license keys 12.1 Text Display Settings on page 114: parameters added due to new corridor display. 21.2 Switch Software on page 164: description of "Keep prev, settings" added.
G	15 May 2012	Updated: 7.12 Setting License Number for Unite CM on page 89: note regarding that no reboot of Unite CM is required if upgrading the number of users. 4.10.1 Add Alarm Actions on page 45: Activation of PTT in loudspeaking mode added. Screenshots also updated. 21.2 Switch Software on page 164: note regarding factory default settings added. 21.3.1 Install New Software in a Redundant System on page 166 24.4.2 Troubleshooting Guide for Unite CM on page 215: troubleshooting for Advanced Diversion added. Appendix B.1: separate cables for DCT1800 and DCT1900. Added: 4.8.4 Input Activity Distribution on page 43 6 Device Configuration on page 74 7.5 Unlock GUI Managed by Unite AM on page 84 15.3.4 SMS Character Set on page 131. Appendix B.5 Appendix K Appendix L

Version	Date	Description
H	27 November 2012	**Added**: 4.6 Import an ESS Backup File on page 35 4.1.2 Add messaging users for paging on page 21 7.1.1 Hostname Setting in Fault Handler E-mail on page 79 15.2 Mixed DECT Systems on page 126 20.6 Add S900 Composite Category for Multi-Site Paging on page 162 15.4.3 Absence Status for Offline Devices on page 132 Appendix M: Multiple Event Handlers on page 261 **Updated**: 2.4 Basic Configuration Steps on page 11: described that the module key is shown in the wizard. 4.1 Add Users to Unite CM on page 20 4.3.2 Multicast Group on page 31: clarified that a handset can be a member in maximum 8 Multicast groups. 4.7 Manage Central Phonebook Entries on page 38, 4.9 Alarm Handling on page 44, 8.2 Customize the Search Result Text on page 91, and 19.2 Create and Send Messages via NetPage on page 148: supported character encodings added. 4.9 Alarm Handling on page 44: clarified the difference between the BAM and Event Handler. 4.11.6 Duty Assignment on page 58: note regarding that maximum 6 000 duty assignments can be added. 9.1.1 ESPA Protocol In on page 101: clarified that two ESPA systems can be connected simultaneously. Change Absent Status on page 64: note regarding absence status for offline handset added. 14.2.1 SMTP Input Interface (receive e-mail as message) on page 121: parameter "IP Address of Event Handler" added. 15.3.3 DECT Message Distribution on page 130: described that port 1817 is required if encrypted DECT is used. 15.4.1 Absence List on page 132: clarified the absence statuses. 18 System 900 Interface on page 139: examples of configuration added. 19.2.4 Message History Status on page 149: described which absent status that is supported by Netpage. 22.2.6 Translation of the User Interfaces on page 176 and Example GUI index4 (default NetPage User Interface) on page 177: described that the NetPage GUI for example can be translated into Russian. 24.4.2 Troubleshooting Guide for Unite CM on page 215: Updated troubleshooting for Group Messaging, Fault Action Handler and BAM used in a multi-site number plan system. Message Action on page 193 and Select Type of Action on page 47: note added regarding Call ID.

Version	Date	Description
(contin.)		Appendix L: Services in Unite CM on page 259: description and configuration examples added. B.5 Cables for Modems on page 230: wiring diagram for 25-pin modem updated. **Removed**: 4.14.6 Deactivate Module Redundancy on page 70: removed first bullet regarding "if redundancy temporarily was deactivated in to order upgrade software..." 25 Related Documents: Ascom 9d documents removed
I	06 March 2013	Added: 4.17 Selection of Data Storage on page 72 6.2.2 Fixed IP-DECT Devices on page 75 6.5 Online Status Report Time for Fixed IP-DECT Devices on page 77 7.4.1 Serial IP Server Protocol on page 84 Updated: 1.1.3 Other additional Licenses on page 2: updated that the Device Manager supports up to 10 000 devices. 4.1.3 Import users from a CSV file on page 22: updated that existing Users and Group can be included in a template. 4.11.2 Action Handler on page 52: "Forced sound indication" parameter added. 4.14.3 Module Redundancy Test on page 68 and 4.14.5 Fallback to the Primary Unite CM on page 70: Note regarding Device Manager added. 6.1 Device Management Setup on page 74: Examples added. Clarified how the fields shall be filled in depending on which devices that shall be managed in Device Manager. Appendix K: Ascom Unite Application Manager on page 258: added that Groups, Mulitcast groups and Broadcast groups can be managed from Unite AM.

Appendix A: Used IP Ports

Port	Application or unit	Transport protocol
20–21	FTP traffic (inbound) outgoing traffic	TCP
25	Simple Mail Transfer Protocol (SMTP)	TCP
53	Domain Name Server (DNS)	UDP
68	DHCP	UDP
80	Web traffic (HTTP)	TCP
113	Authentication for mail server	TCP
123	Time synchronisation (NTP)	UDP
162	Simple Network Management Protocol (SNMP)	UDP
443	Web traffic (HTTPS)	TCP
10132-10135	GUI for Duty assignment, Action configuration and Event assignment	TCP
10141	WLAN messaging interface	TCP
1200	Alcatel Omni PCX Enterprise	TCP
1321–1322	OAP Server	TCP
1814–1817	MX-ONE/MD110/IP-DECT/EMN	TCP
2775	Phonebook Service	UDP
3217	Unite traffic	UDP
5891	Netpage	TCP
8080	Web traffic (HTTPS)	TCP
10089	Ascotel IntelliGate	UDP
10101	Remote connection - TCP and RS232 conversion	TCP
10103	Remote connection - Communication between Remote Access Client and Remote Access Server	TCP
10130	Applet communication (Activity Log Viewer)	TCP
10141	Netwise presence management system	TCP
10147	DECT Charger Communication	TCP
10153	Device Manager Communication	TCP
33000–33001	WLAN messaging interface	TCP
45000–45400	FTP traffic (outbound) incoming traffic	TCP

Appendix B: RS232 Connections

B.1 Cables for DCT1800 and DCT1900

Figure 92. Connection for messaging in DCT1800 and DCT1900 systems.

A cable with RS232 and D-SUB (9-pin female) connectors is required to be able to transmit messages to handsets and to receive messages, data and alarms from the handsets. The cable should be connected to the COM1 port on Unite CM and to the Printer (PR) port on the Radio Exchange. To be able to configure DCT1800/DCT1900 remotely via a Unite CM, this type of cable should also be connected between the COM2 port on Unite CM and the PC port on the Radio Exchange.

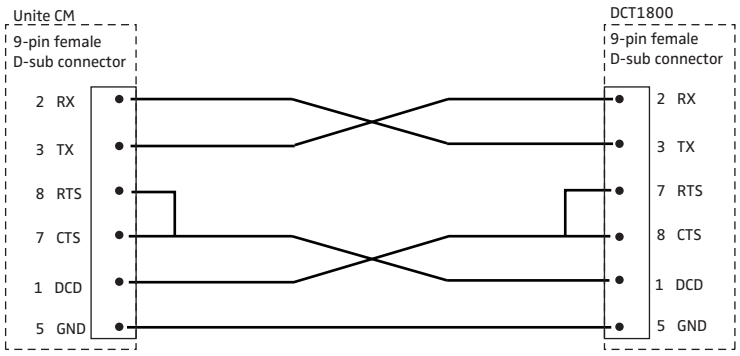


Figure 93. Cable wiring for DCT1800

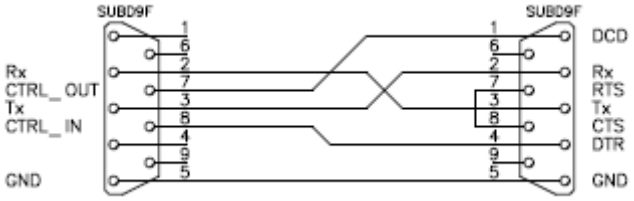


Figure 94. Cable wiring for DCT1900

B.2 Cables for BusinessPhone

Unite CM and the BusinessPhone have to be connected in order to be able to transmit messages to handsets and to receive messages, data and alarms from the handsets. The cable should be connected to the COM1 port on Unite CM and to the I/0 port on the IC-CU2 board in the BusinessPhone. The cable should be wired as described below.

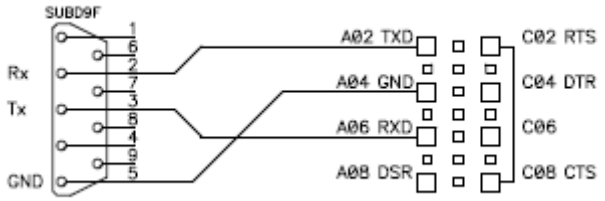


Figure 95. Cable wiring for BusinessPhone

To be able to configure BusinessPhone remotely via a Unite CM, a second cable is required. It should be wired as described above and connected between the COM2 port on Unite CM and the Maintenance port on the IC-CU2 board in the BusinessPhone.

B.3 Cables for the ESPA-, the Ascom Line- and the TAP protocol

Figure 96. Connection to external equipment

A cable with RS232 and D-SUB connectors is required to be able to receive pagings from external equipment. By default the cable shall be connected to the COM2 port on Unite CM for ESPA in, Ascom Line protocol and TAP in and also for ESPA out and TAP out.

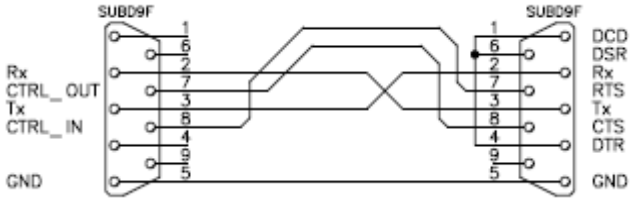


Figure 97. Cable wiring for the ESPA -, the Ascom Line- and the TAP protocol

B.4 Cables for Remote Management Client

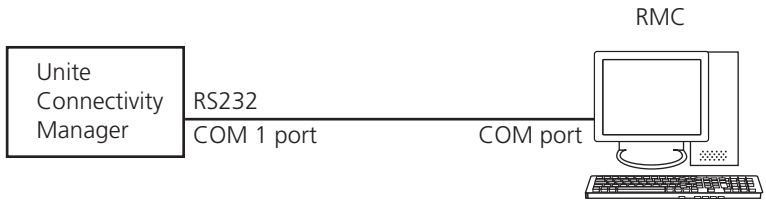


Figure 98. Connection for Remote Management.

A cable with RS232 and D-SUB (9-pin female) connectors is required to be able to manage Unite CM via a Remote Management Client. The cable should be connected to the COM1 port on Unite CM and to a free COM port on the PC.

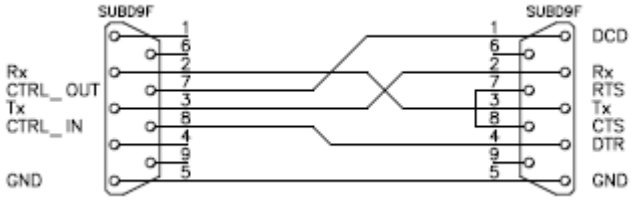


Figure 99. Cable wiring for RMC

B.5 Cables for Modems

A cable with RS232 and D-sub connector is required when a modem shall be connected to the Unite CM.

.

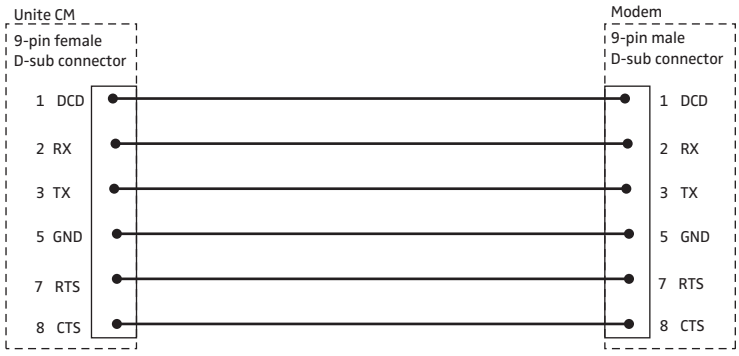


Figure 100. Cable wiring for modem with 9-pin D-sub connector.

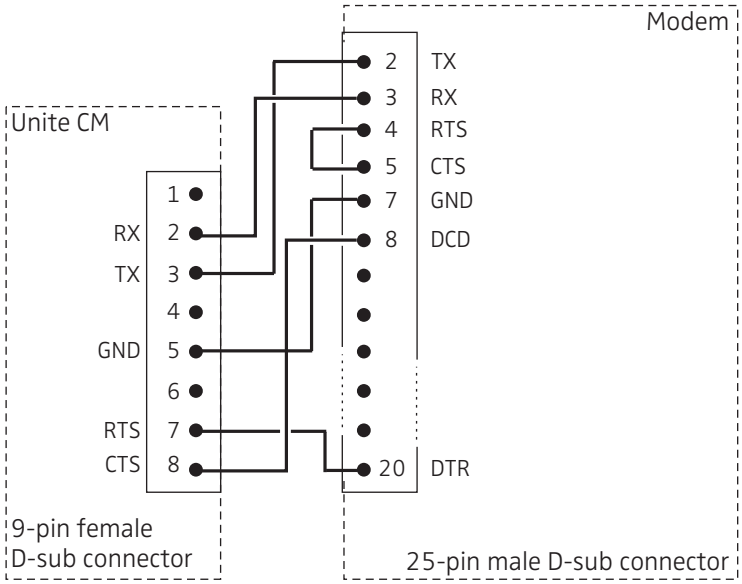
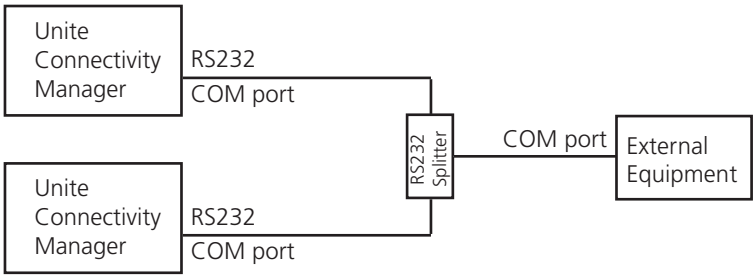


Figure 101. Cable wiring for modem with 25-pin D-sub connector.

B.6 R232 Cable Connections in a Redundant System

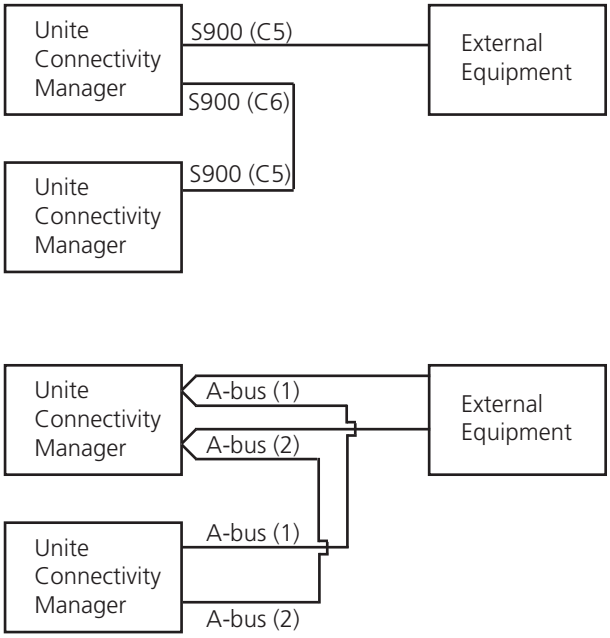
In a redundant system, having equipment connected via serial interface, must the R232 cable be attached to both the primary Unite CM and the secondary Unite CM. By using a RS232 data splitter the cable can be branched to both modules.



Appendix C: System 900 Connections

The external equipment can be connected to the A-bus in two different ways depending on the connector used.

C.1 System 900/A-bus Connections in a Redundant System



Appendix D: Network Monitoring in a Redundant System

In a redundant system, both the primary Unite CM and the secondary Unite CM can check if they have connection to the network by sending ICMP inquiries to an optional equipment in the same network. It is recommended to use the equipment that is centrally installed in the network, for example an IP-PBX. See the example below for more information.

If the active Unite CM loses the connection to the network, the standby Unite CM will become active instead.

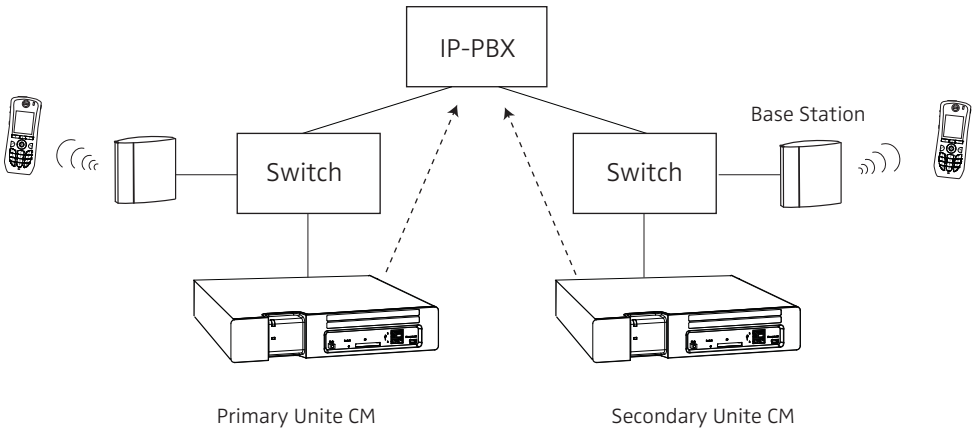


Figure 102. Illustration of using a centralized equipment as network reference

In Figure 88, both the primary Unite CM and the secondary Unite CM are using the IP-PBX as network reference since it is centrally installed in the network.

NOTE: The use of the network monitor function is optional[1], but it is strongly recommended to use when the modules are connected to different switches. If the function is disabled and the modules cannot communicate with each other, both modules might become active since they consider that the other module has failed. The result is that the one part of the system will write data to the primary Unite CM, and the other part will write data to the secondary Unite CM. This behaviour is called ''split brain behaviour''.

1.By setting the *Network monitor IP address* to 127.0.0.1 disables the function.

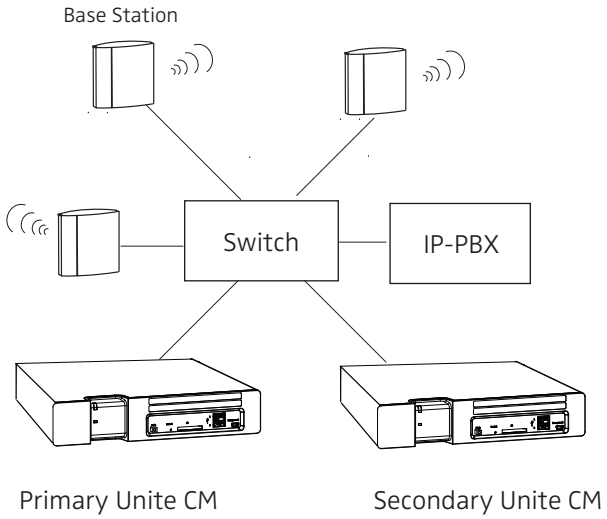


Figure 103. Illustration of a network where no network monitoring is required.

If the primary Unite CM and secondary Unite CM are connected to the same switch (see Figure 89), no equipment (for example an IP-PBX) is needed as network reference. If the secondary Unite CM do not receive any response from the primary Unite CM, the primary Unite CM has actually failed and the secondary Unite CM becomes active.

Appendix E: Fault Handling Configuration Example

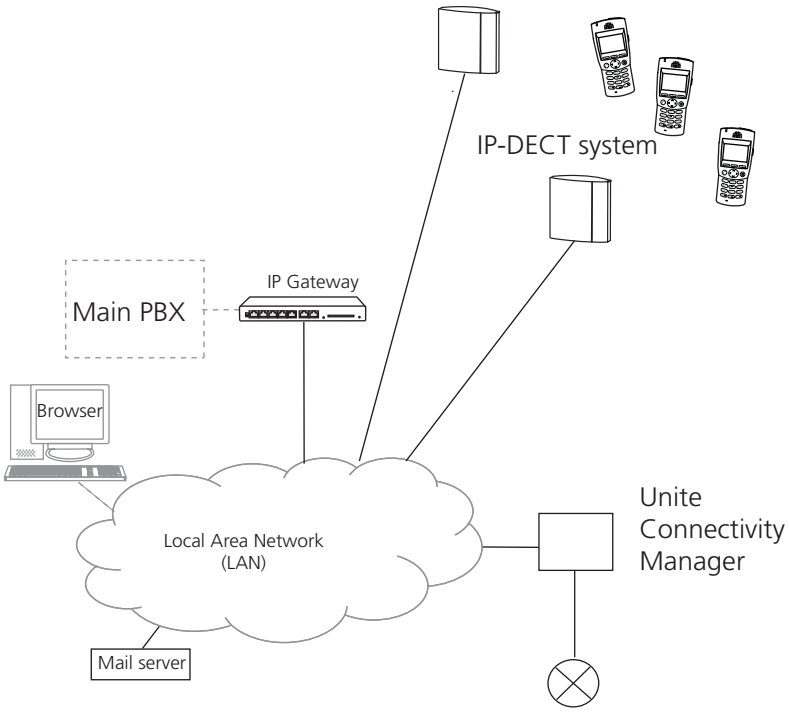


Figure 104. Unite CM fault handling in an IP-DECT system installation.

This example shows a Unite CM connected to an IP-DECT System. A lamp is connected to Unite CM error relay and Unite CM is configured to activate the error relay and light the lamp for 60 seconds when a DECT error is reported.

NOTE: When module redundancy is activated (see 4.14 Module Redundancy on page 65), the error relay should only be connected to the primary Unite CM since it is preferred to be the active module.

For extra security, Unite CM is also configured to send an e-mail to a user in the system.

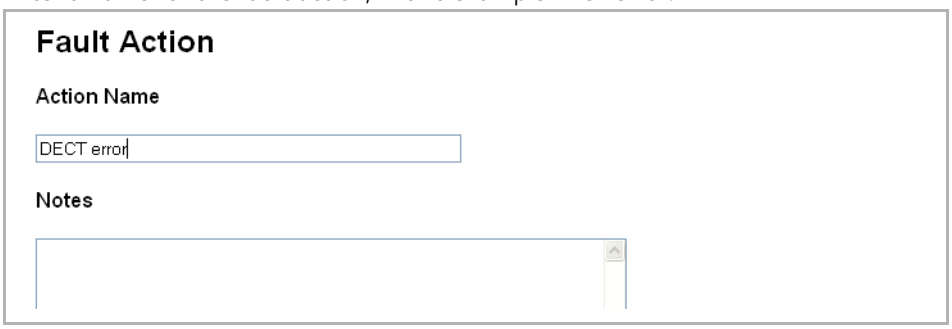
NOTE: Requires an additional license, see 1.1 Licenses for Unite CM on page 1 and that the mail server IP address has been set in the wizard.

Settings

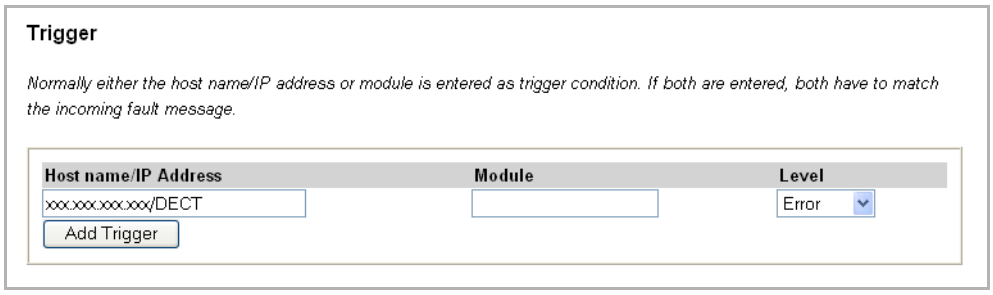
The actions are set up to trigger when Unite CM detects an error on the connection to the IP-DECT system. The actions on the triggers are to light a lamp and to send an e-mail.

1 Select Fault Handling > Fault Actions in the menu on the *Configuration* page.

2 Enter a name for the fault action, in this example DECT error.

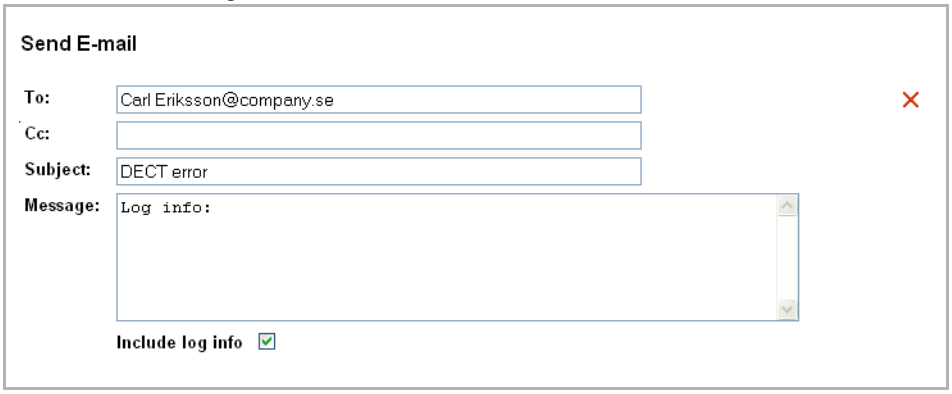


3 Enter the Unite CM IP address "xxx.xxx.xxx.xxx/DECT" as trigger condition, where xxx.xxx.xxx.xxx is the IP address.

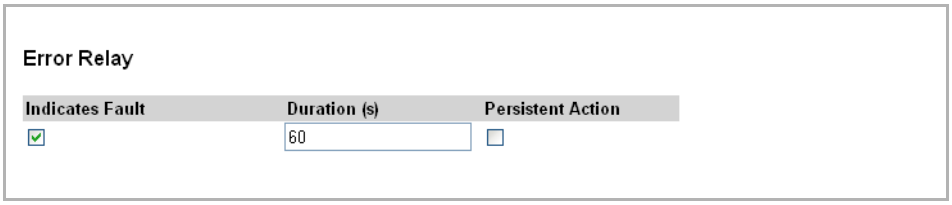

Trigger
Normally either the host name/IP address or module is entered as trigger condition. If both are entered, both have to match the incoming fault message.
Host name/IP Address
Module
Level
xxx.xxx.xxx.xxx/DECT
Error
Add Trigger

4 Select the error level to trigger on as "Error".

5 Select the action Send E-mail and enter the complete e-mail address to the recipient. Select the Include log info check box.



6 Mark the Error Relay "Indicates Fault" check box to use the output/relay to indicate fault. Set the duration to 60 s.



7 Click ''Save''.

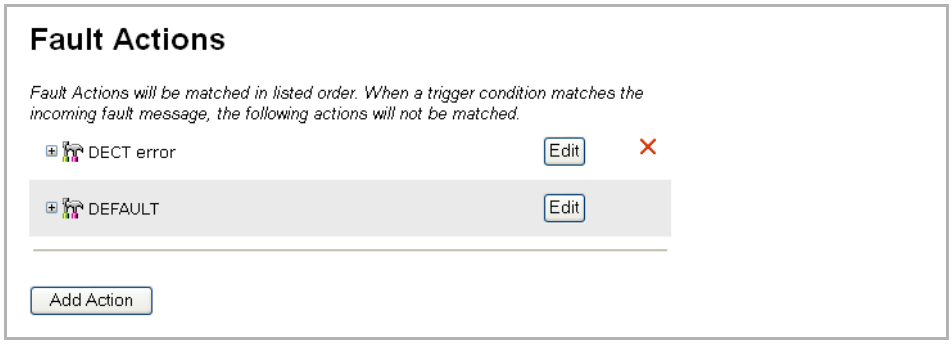

Fault Actions
Fault Actions will be matched in listed order. When a trigger condition matches the incoming fault message, the following actions will not be matched.
DECT error
Edit
DEFAULT
Edit
Add Action

Figure 105. The action list with the DECT error action.

Unite CM is now configured to light the lamp connected to the error relay and to send an e-mail with the log files, to someone responsible for the system in case of error.

Appendix F: Alarm Action Configuration Examples

This appendix presents examples on how alarm actions can be configured.

System setup for examples

In this section, first the included system components are presented, then which inputs and outputs that need to be setup.

System Components

- One Alarm Module.
  4 inputs has been defined in the Input/Output Setup.
  Input names:
  - Cold-storage, door open
  - Cold-storage, door still open
  - Cold-storage, door open very long
  - Cold-storage, door closed
- One Output Module.
  2 outputs have been defined in the Input/Output Setup.
  Output names:
  - Cold-storage lamp
  - Siren
- 4 handsets with push-button alarms.
  handset addresses:
  1440, 1441, 1442 and 1443.

Input/Output Setup

In these examples, the outputs and inputs are set according to the following figure.

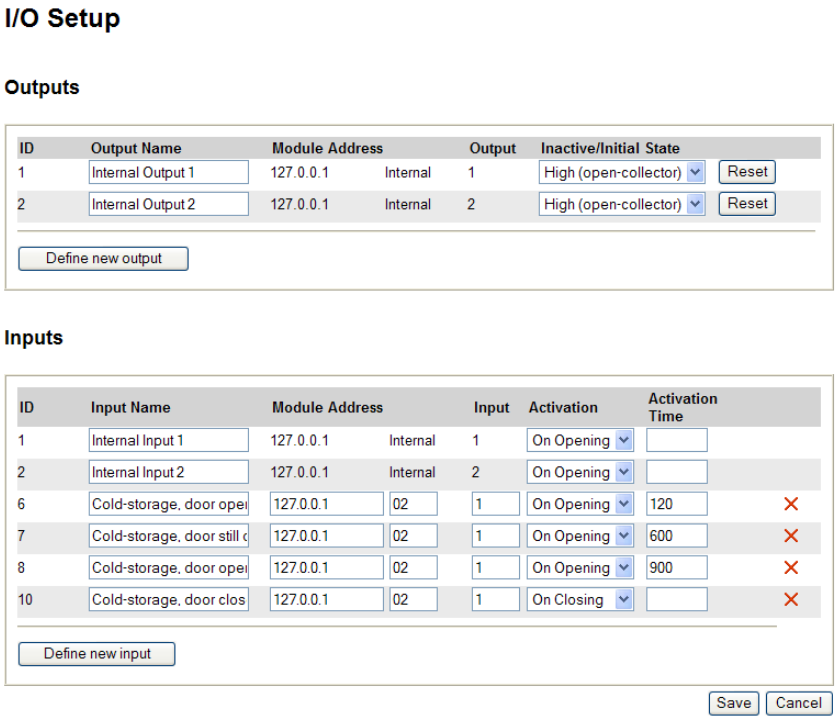


Figure 106. I/O setup.

Example 1

A push-button alarm (double press) is received from 1440. A message is sent to the other handsets and a siren starts to sound. The alarm is cancelled by sending the data 1440 and then the siren stops.

Two alarm actions are created. One that handles the push-button alarm called ''Push-button alarm from 1440'' and one that handles the cancellation called ''Alarm cancellation''.

Push-button alarm from 1440

Select Alarm handling, Alarm Actions and set Alarm Trigger ''Push-button double press''

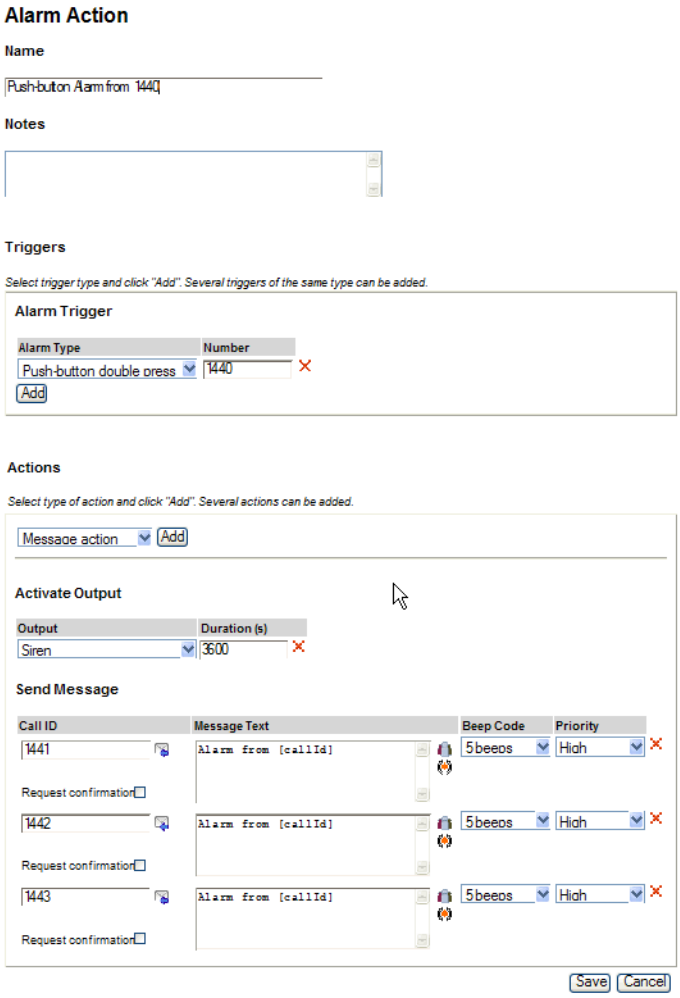


Figure 107. Alarm trigger setup.

Activate Actions

Two different actions are setup, a siren and messages sent to other handsets.

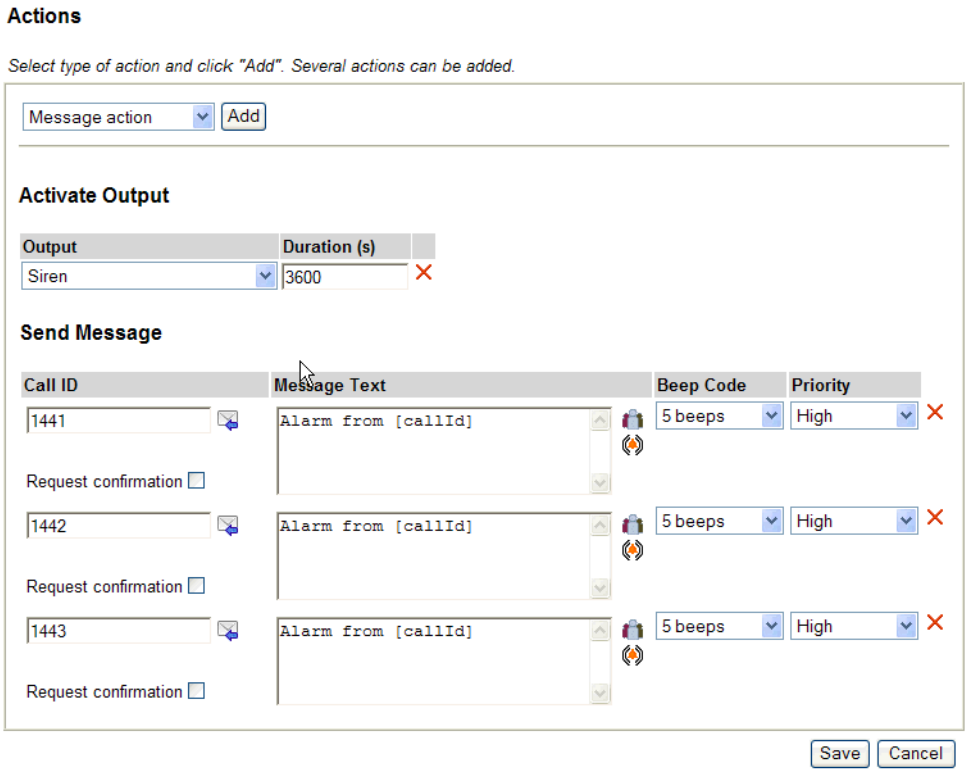


Figure 108. Activated Alarm Actions.

For Output Action Siren, the value is set to max value 3600.

Alarm cancellation

For handset 1440, Alarm cancellation is setup with a Data Trigger with an Alarm with duration of 1 second.

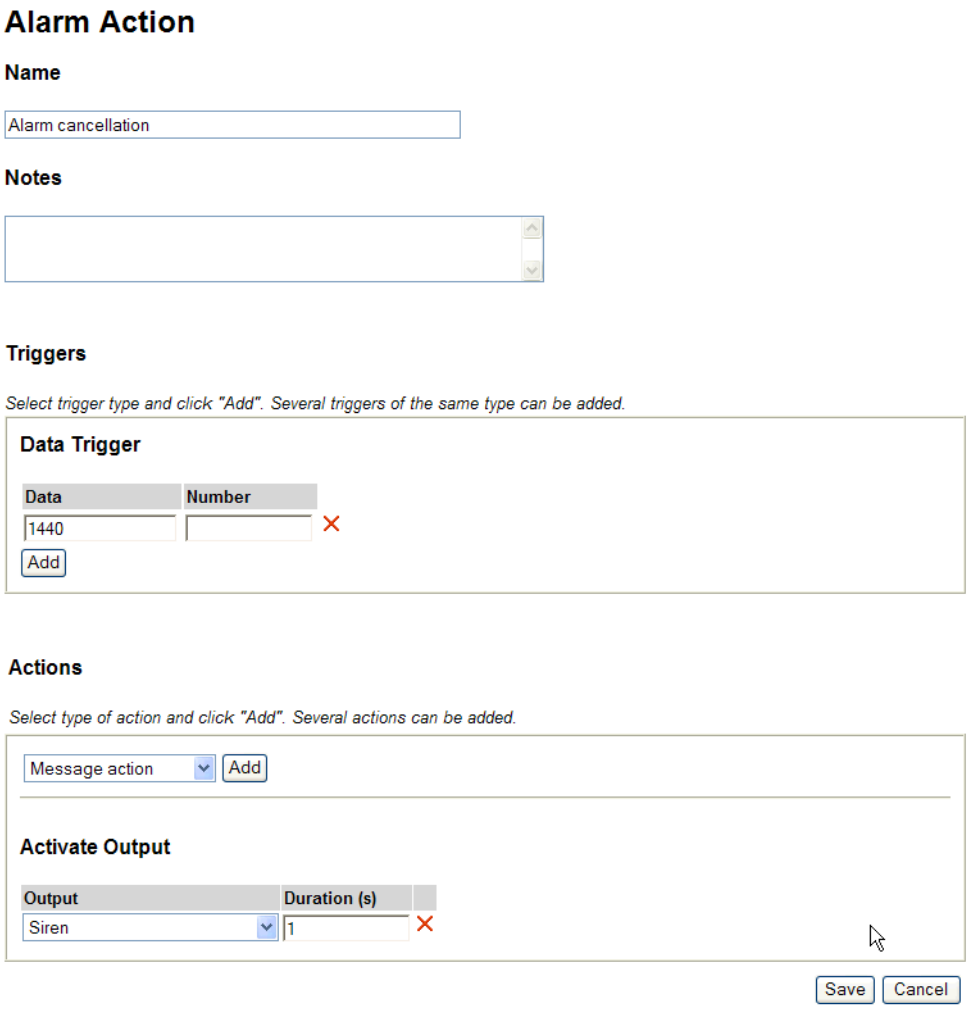


Figure 109. Activating an Action for Alarm Cancellation.

It does not matter which handset that sends the data so the trigger is general when it comes to handset number.

The output is set to the initial state again (after 1 second).

Example 2

When the door to one of the cold-storage rooms opens, the input from Cold-storage room is activated. If the door is open longer than 2 minutes a message is sent and the lamp above the door is lit. If the door still is open after 10 minutes another message is sent. After 15 minutes another message is sent and the siren starts to sound. When the door is closed the siren and lamp are turned off.

Three alarm actions are created. One that handles the alarm called ''Cold-storage room open'', one called ''Cold-store room open very long'' and one called ''Cold-storage room closed''.

Cold-storage room 1, door open

Input Triggers: ''Cold-storage door open'' and ''Cold-storage door still open''

When the door has been open for 2 minutes (120 seconds), the action is started. The action shall not be repeated so the ''Repetition time'' is not stated and the value in the ''Max. No. of Repetitions'' field has no meaning.

When the door has been open for 10 minutes (600 seconds), another message is sent as a reminder. A separate Alarm Action is required if a different beep-code is desired.

Actions Activate Output Action and Send Message Actions

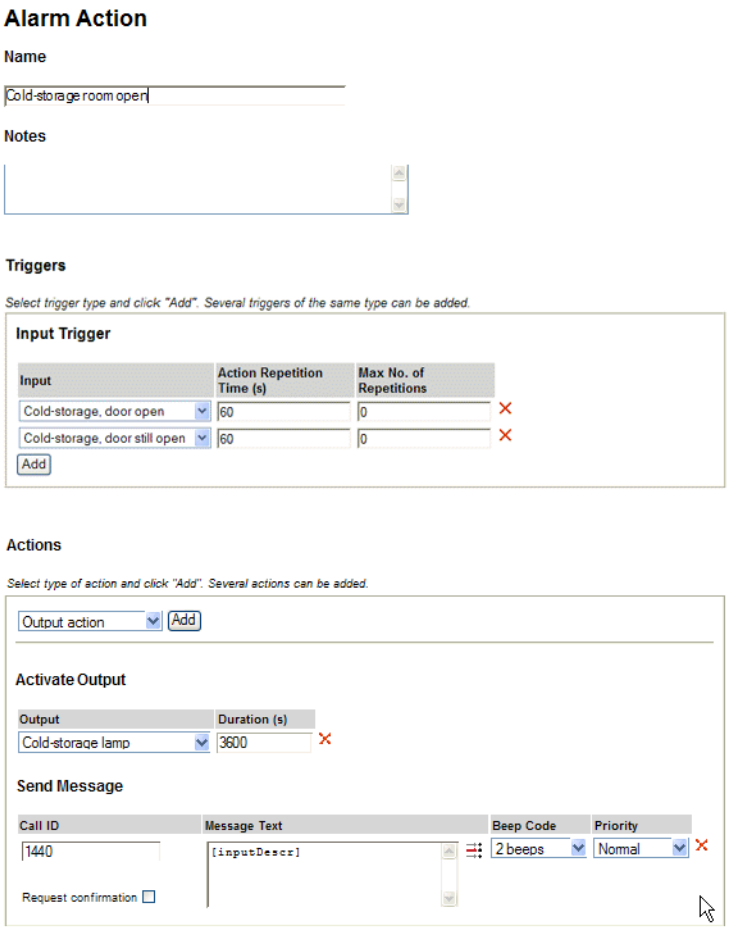


Figure 110. Alarm Action, Cold-storage room open.

For Activate Output Action, the duration is here set to max value 3600.

Cold-storage room 1, door open very long

The Input Trigger ''Cold-storage room, door open very long'' is used.

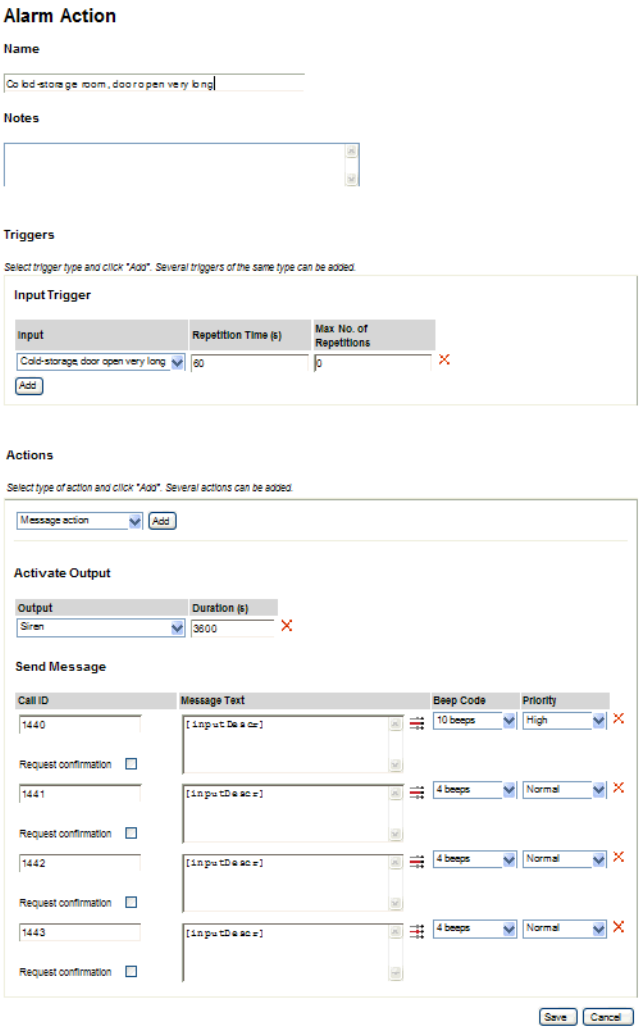


Figure 111. Cold-storage room 1, door open very long.

When the door has been open for 15 minutes (900 seconds), the message is sent to all handsets and the siren starts to sound.

The duration is set to max value 3600 and will sound until expired or another action is started with shorter expire time, for example ''Cold-storage room closed''.

Cold-storage room door closed

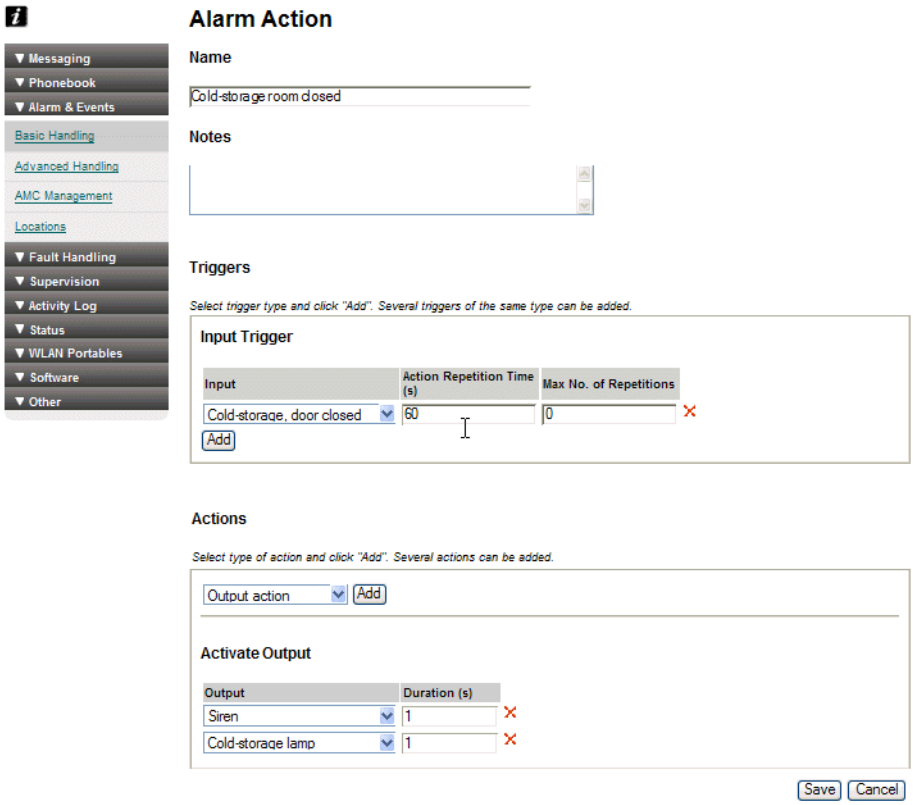


Figure 112. Cold-storage room door closed.

For Input Trigger ''Cold-storage, door closed'': When the door closes the actions are started. The output is set to the initial state again (after 1 second).

Summary of alarm actions

This figure shows a list of the Alarm Action setup in the examples.

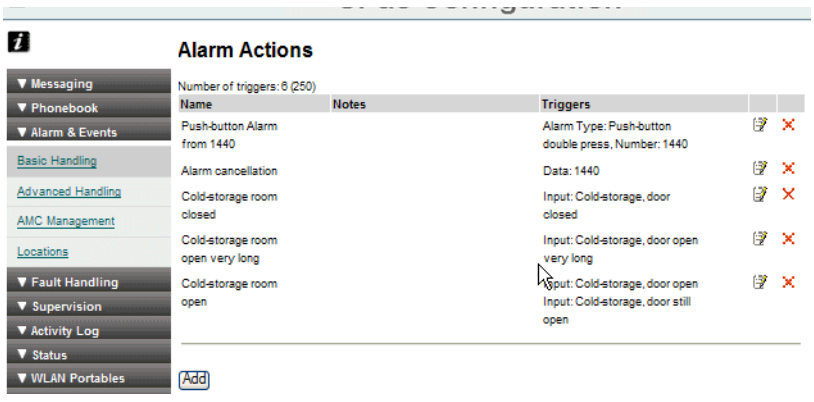


Figure 113. Summary of Alarm Actions.

Appendix G: ASCII-table

ASCII stands for American Standard Code for Information Interchange. The ASCII-table is like a dictionary for translating numbers into characters.

The table below shows the translation of decimal numbers into characters.

Dec.	Char.	Dec.	Char.	Dec.	Char.	Dec.	Char.
0	NUL (null)	32	Space	64	@	96	`
1	SOH (start of heading)	33	!	65	A	97	a
2	STX (start of text)	34	"	66	B	98	b
3	ETX (end of text)	35	#	67	C	99	c
4	EOT (end of transmission)	36	$	68	D	100	d
5	ENQ (enquire)	37	%	69	E	101	e
6	ACK (acknowledge)	38	&	70	F	102	f
7	BEL (bell)	39	'	71	G	103	g
8	BS (backspace)	40	(	72	H	104	h
9	TAB (horizontal tab)	41	)	73	I	105	i
10	LF (NL line feed, new line))	42	*	74	J	106	j
11	VT (vertical tab)	43	+	75	K	107	k
12	FF (NP form feed, new page)	44	’	76	L	108	l
13	CR (carriage return)	45	-	77	M	109	m
14	SO (shift out)	46	.	78	N	110	n
15	SI (shift in)	47	/	79	O	111	o
16	DLE (data link escape)	48	0	80	P	112	p
17	DC1 (device control 1)	49	1	81	Q	113	q
18	DC2 (device control 2)	50	2	82	R	114	r
19	DC3 (device control 3)	51	3	83	S	115	s
20	DC4 (device control 4)	52	4	84	T	116	t
21	NAK (negative acknowledge)	53	5	85	U	117	u
22	SYN (synchronous idle)	54	6	86	V	118	v
23	ETB (end of trans. block)	55	7	87	W	119	w
24	CAN (cancel)	56	8	88	X	120	x
25	EM (end of medium)	57	9	89	Y	121	y
26	SUB (substitute)	58	:	90	Z	122	z
27	ESC (escape)	59	;	91	[	123	{
28	FS (file separator)	60	<	92	\	124	|
29	GS (group separator)	61	=	93	]	125	}
30	RS (record separator)	62	>	94	^	126	~
31	US (unit separator)	63	?	95	_	127	DEL

Appendix H: Extracting Information from HL7 v2 Messages

The appendix describes how to configure the Event Handler for extracting information from HL7 version 2 messages into event elements for event assignment.

The HL7 version 3 is an XML based protocol. See Appendix I: XML Message Handling in Event Handler for more information.

H.1 HL7 Classic Style Message Definition

The HL7 protocol transfers simple messages, in which all data is transferred as ASCII data. A message is terminated with the characters as defined in the Minimum Lower Level Protocol (MLLP).

Each segment begins with a three-character literal value that identifies it within a message. A segment is always terminated with an ASCII Carriage Return character. Segments may be defined as required or optional and may be permitted to repeat.

The first segment is a message header (MSH). It contains the delimiter characters to be used in the message (|^~\&) and other information. Each segment consists of several Data fields. Data fields are separated with a vertical bar character '|'. Individual data fields are found in the message by their position within their associated segments. A data field can consist of more than one component. A component may have sub components. Fields may be repeated.

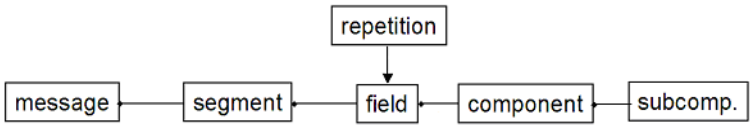


Figure 114. A HL7 message.

Delimiters ASCII

- VT = 11 (0x0B)
- FS = 28 (0x1C)
- CR = 13 (0x0D)

HL7	Define by	Suggested value	Comment
Message	MLLP	start: <VT> stop: <FS><CR>	Defined in TCP connection parameters for the HL7-MLLP TCP connection in the ASCII Input Module
Segment	HL7	stop: <CR>	Defined static in Event Handler configuration
Field	1st char after "MSH" segment ID	'|' bar	Defined by HL7 message received by Event Handler.
Repetition	3rd char after "MSH" segment ID	'~' tilde	Defined by HL7 message received by Event Handler.
Component	2nd char after "MSH" segment ID	'^' circumflex	Defined by HL7 message received by Event Handler.

Sub-component	5th char after ''MSH'' segment ID	'&' ampersand	Defined by HL7 message received by Event Handler.
Escape	4th char after the ''MSH'' segment ID	'\' backslash	To escape the above defined message element delimiters when used in fields represented by string/text data types. Defined by HL7 message received by Event Handler.

H.2 Example HL7 v2.x

Through this document the following HL7 v2 example message with the MSH, EVN, PID, PV1, IN1 and IN2 segments encapsulated in a MLLP session will be used:

- MSH – Message Header
- EVN – Event type
- PID – Patient Identification
- PV1 – Patient visit
- IN1 – Insurance
- IN2 – Insurance additional information

```
<VT>MSH|^~\&|HIS|ADT_MODULE|ASCOM|UNITE|20060109024819||ADT^A08
|20060109024311170|P|2.2|||AL|SU||
EVN|A08|200601090243|<CR>
PID|||2490298||Långstrump&&Långstrump&Mr.&Nilsson^Pippi^Viktual
ia Rullgardina Krusmynta
Efraemsdotter^^Ms.^""~Langkous&&Langkous&Dhr.&Nilsson^Pippi^Vic
tualia Rolgordijna Kruizemunta
EfraÏmsdochter^^Juffrouw^""||19630122|M|||Villa Villekulla
Bråkmakargatan^7^Vimmerby^^SE-
9999||0046123456789|||""|""|||||||N||""<CR>
PV1||O|First aid^Room 5^Bed
2|||^^|""^""^""^""^^""^""||||||||||""||||||||||||||||||""|""||
|||||""|<CR>
IN1|1||7022|CZ Zorgverzekering|Postbus^99999^Tilburg^^9999
AB||076-5243xxx|||||||P|||||||||||||||||||900080820<CR>
IN2|||||||||||||||||||||||||||3|H<CR>
<FS><CR>
```

H.3 Event Handler Configuration

This section describes how an HL7 v2 message is transmitted from the Hospital Information System (HIS) to the Unite CM system.

HIS - ASCII

The Hospital Information System (HIS) connects to Unite CM\ASCII through a TCP/IP socket. The IP address to connect to is the IP address of the Unite CM module. An HL7 application message is sent over this connection. The message is encapsulated between the input start and input stop characters, see the figure in H.4 Configure Unite CM on page 250.

The ADT is a software module in HIS.

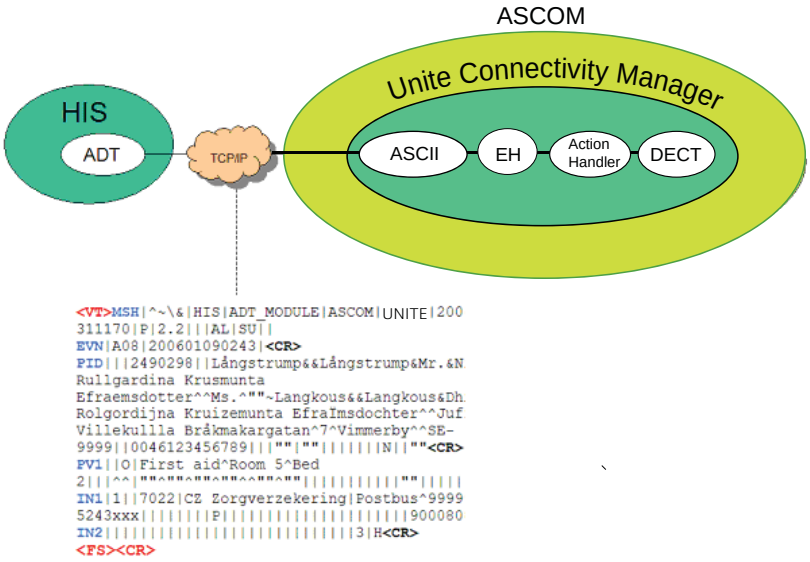


Figure 115. The connection between ADT - ASCII.

ASCII - Event Handler

The ASCII application will send a UNITE paging message to the Event Handler. The body of the paging message includes the encapsulated message.

NOTE: The paging body text can only contain up to 5000 characters.

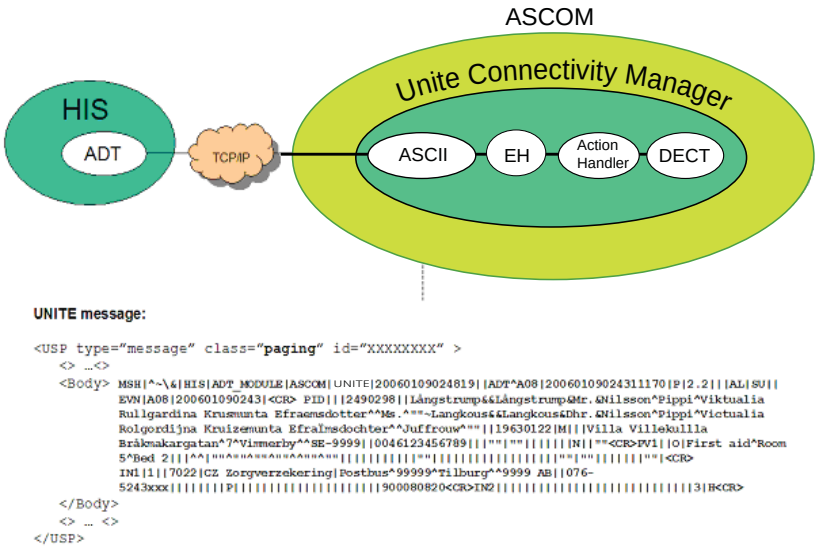


Figure 116. Paging message to the Event Handler.

Event Handler - Action Handler

Based on a translation table that is defined by the customer, the Event Handler will extract the needed information from the paging body text and send that as event elements to the Action Handler.

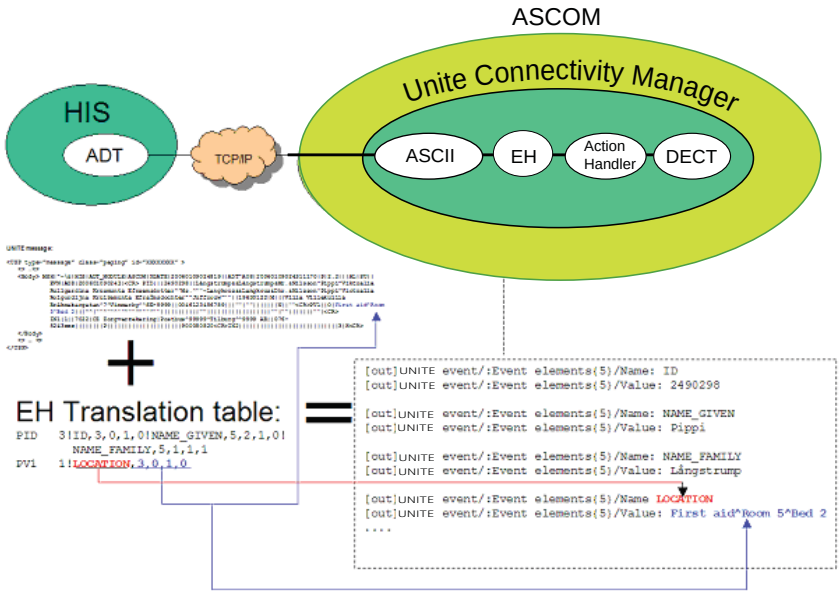


Figure 117. Event Handler translation table.

Acknowledgements

In HL7 two types of acknowledgements exist. Accept and Application acknowledgement. The MSH segment of the received HL7 message defines which type of acknowledgment the sending party expects. This EH configuration is build to only send 'accept' on both types of acknowledgements. This EH configuration will not send 'error' or 'reject' for those two types of acknowledgements. A customer who would like this functionality needs to extend the configuration himself.

Depending on the values of Fields 15 and 16 of the MSH segment an acknowledgement type is expected.

The EH configuration will always send:

- Accept acknowledgement with value CA ''commit accept'' when MSH field 15 has a value of AL (always) or SU (success completion)
- Application acknowledgement with value AA ''application accept'' when MSH field 16 has a value of AL (always) or SU (success completion)

- When MSH fields 15 and 16 both are omitted, only an application acknowledgement with value 'AA' will be send.

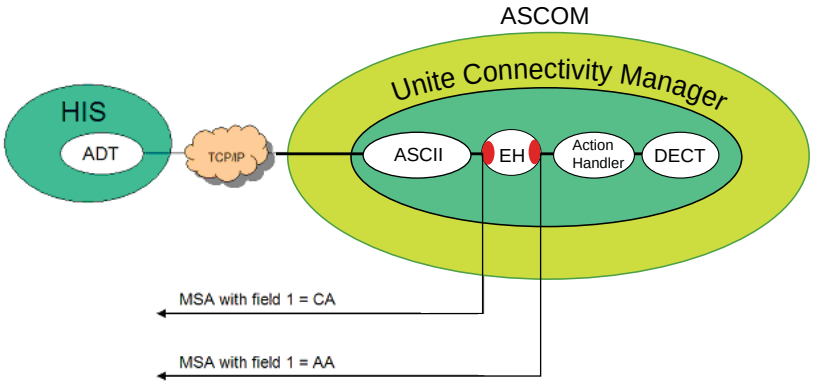


Figure 118. Two different acknowledgments.

The Commit Accept acknowledgement will be send as soon as the Event Handler starts to process the HL7 message. The application acknowledgement will be send as soon as the event elements are sent to the Action Handler.

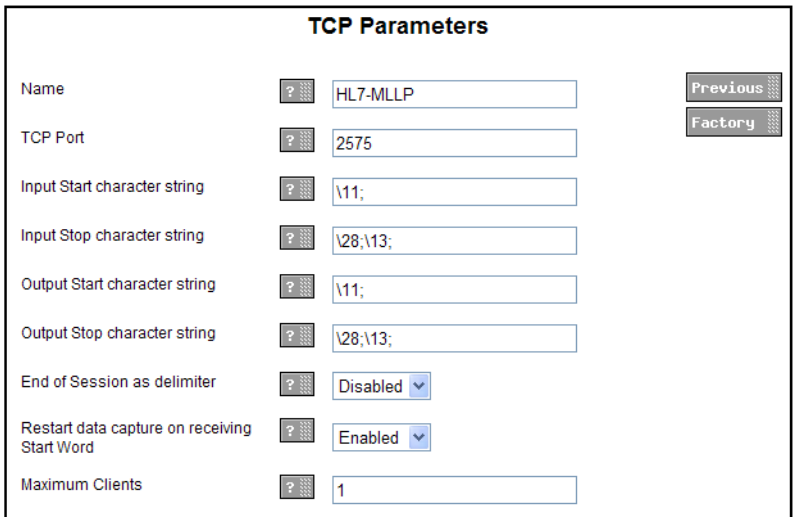
H.4 Configure Unite CM

ASCII Input Interface

The ASCII input interface is configured for Minimum Lower Level Protocol (MLLP) session control over a TCP connection on port 2575 (HL7 port, registered at www.iana.org).

1 On the *Advance Configuration* page, select ''ASCII'' to edit the configuration.

2 If a HL7 port already is configured in TCP Server Parameters, click ''HL7-MLLP'' or similar to verify your settings. Otherwise, click ''NOT USED''.



3 Enter the parameters according to figure above.

H.5 Load the HL7 v2 Translation Table

The translation table is the link between a HL7 style message and the Event Handler in Unite CM. A default translation table is included in the Unite CM. The translation table is defined/ modified by the customer.

This instruction describes how to load the HL7 default translation table.

1 Click ''Configuration'' on the start page.

2 Select Alarm & Events > Advanced Handling in the menu on the *Configuration* page.

3 Click ''Administration''.

4 Click ''Load HL7 version 2'' to load the sample database.

5 Click ''Translation Tables'' to open the Event Handler Configuration page.

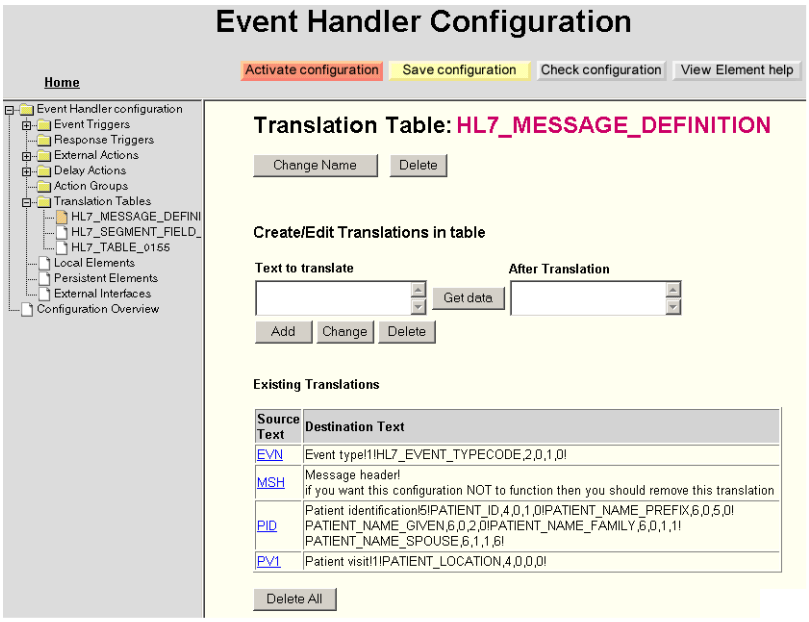


Figure 119. HL7 Translation Table v2.

For more information on how to create/edit a translation table, see Programming Guide, Event Handler, TD 92329GB.

For information on Source text from HL7, see an applicable HL7 document.

Define HL7 v2 Segment Data

The source text is used to indicate from which HL7 segment data needs to be extracted. The destination text defines what data is extracted from the segment and how the event element will be named. They are defined as:

- Source text = HL7 segment ID as defined by the standard (for example PID)
- Destination text = <description>!<number of values>!<ELEMENT_TO_EXTRACT>

Where:

- number of values = number of ELEMENT_TO_EXTRACT occurrences that follows in this definition.

- ELEMENT_TO_EXTRACT = [<ELEMENT NAME>,<FIELD>,<REPETITION>, <COMPONENT>,<SUBCOMPONENT>]

Where:

- ELEMENT_NAME = Name of the Event element that is sent to the Action handler
- FIELD = Field number that includes the data (start count from segment ID)
- REPETITION = Repetition number of the field that includes the data (EH will take first occurrence if no repetition exists)
- COMPONENT = Component number of the field that includes the data
- SUBCOMPONENT= Subcomponent number of the component that includes the data (EH will take COMPONENT if no subcomponent exists)

Example:

Note: A zero (0) is used if only one (1) value exist in the segment.

PID Patient Identification!3!ID,4,0,0,0!NAME_GIVEN,6,1,2,0!NAME_FAMILY,6,1,1,1

Would extract the following 3 elements from the PID segment from example message:

- Element name = ID, with value = 2490298
- Element name = NAME_GIVEN with value = Pippi
- Element name = NAME_FAMILY with value = Långstrump

Note: Do NOT remove or change the MSH entry in the translation table. It is mandatory for the Event Handler configuration to work properly.

Appendix I: XML Message Handling in Event Handler

The appendix describes how to define segment from XML messages. Unite CM includes a protocol template that can be used as an example for XML messages received by event handler from external systems.

XML messages are written as:

```
<tag>
   value
</tag>
```

I.1 Example XML message

The following example XML message is used to explain the XML protocol template delivered with Unite CM:

```
<Message>
  <Type>PSPA</Type>
  <PSPA>
    <Patient>
      <Id>1234567890</Id>
      <Name>
        <Prefix>Miss</Prefix>
        <Given>Pippi</Given>
        <Family>Langkous</Family>
      </Name>
      <Location>
        <Ward>
          <Name>First-aid</Name>
        </Ward>
        <Room>
          <Name>-R1</Name>
        </Room>
        <Bed>
          <Name>-S4</Name>
        </Bed>
      </Location>
    </Patient>
  </PSPA>
</Message>
```

I.1.1 Define XML Segment Data

The translation table is defined as: The source text must be an incrementing number indicating an index to each element that needs to be extracted from the XML message. The destination text defines which tag values are extracted from the XML document.

- Source text = incrementing number starting at 1
- Destination text = <ELEMENT_NAME>!<Xpath expression>

Where:

- ELEMENT_NAME= Name of the Event element that is sent to the Action handler
- != a mandatory delimiter that is needed by the event handler configuration

- Xpath expression= an expression that defines which tag values to include in the element value

The example translation table:

1 PATIENT_NAME!/Message/PSPA/Patient/Name

2 PATIENT_LOCATION!/Message/PSPA/Patient/Location

3 XML_EVENT_TYPECODE!/Message/Type

Would result in the following event elements:

- [out]Unite_CM event/:Event elements{1}/Name: PATIENT_NAME
- [out]Unite_CM event/:Event elements{1}/Value: Miss Pippi Langkous

- [out]Unite_CM event/:Event elements{2}/Name: PATIENT_LOCATION
- [out]Unite_CM event/:Event elements{2}/Value: First-aid-R1-S4

- [out]Unite_CM event/:Event elements{3}/Name: XML_EVENT_TYPECODE
- [out]Unite_CM event/:Event elements{3}/Value: PSPA

Note: The left row of the translation table must be incrementing starting at 1. It is mandatory for the Event Handler configuration to work properly.

The XML syntax in received data must be correct for the template to work. If the received data includes non-XML data it must first be removed.

I.1.2 Consideration

- Unite CM supports the XML Path Language (XPath) 1.0 from Nov. 16 1999 (see www.w3.org/TR/xpath for a specification).

Appendix J: Protocol Limitations (input)

This appendix describes a number of protocol specific limitations and deviations and is valid for input direction. The serial interface included in Unite CM is a successor to the system 900 module S942SI Serial Interface and the supported protocols are described in the document Protocol, Serial Data Interface S942SI, TD 92088GB. To be able to fully understand the limitations it is recommended to have this document available.

J.1 ESPA 4.4.4

J.1.1 Functionality

The protocol consists of blocks which consist of records which consist of data.

J.1.2 Limitations

Protocol Blocks

The original ESPA 4.4.4 specification has 4 different blocks and an additional 5'th block for equipment manufacturer specified functionality. The 5'th block is not used by Ascom and Ericsson dialect, instead two additional blocks 7 and 9 are specified for the dialects.

Request for license (Block 7, Ascom and Ericsson dialect):	This block is not supported since license handling differs from how it was done in 942SI. The block is NAK:ed if received.
Request for module key number (Block 9, Ascom and Ericsson dialect):	This block is not supported since license handling differs from how it was done in 942SI. The block is NAK:ed if received.

Protocol Records

Call type: Speech call (Record 4.2):	Speech paging is not supported. This record is handled as a standard paging (Record 4.3)
Call type: Remote ack of old paging in mobile unit (Record 4.5, Ascom dialect):	This record is NAK:ed since it is not supported by Unite.
Call type: Erase of old paging (Record 4.6, Ascom dialect):	If neither ''ID'' (Record 9) or ''Running Number'' (Record D) is included in the message, the message is NAK:ed. In 942SI it was ACK:ed but didn't function.
Call type: Cordless phone, undefined type (Record 4.7, Ascom dialect):	Sent as standard paging (Record 4.3).
Call type: Cordless phone, internal type (Record 4.8, Ascom dialect):	Sent as standard paging (Record 4.3).
Call type: Cordless phone, external type (Record 4.9, Ascom dialect):	Sent as standard paging (Record 4.3).

Number of transmissions (Record 5, standard ESPA):	This record is accepted but ignored since it is not supported by Unite. Number of transmissions can be set under System 900 and is then valid for all messages independent of the record value. Here it is also possible to determine number of transmissions based on the paging priority (advanced).
Mailbox number (Record A, Ericsson dialect):	This record is accepted but ignored since it is not supported by Unite.
Infopage (Record C, Ascom dialect):	This record is accepted but ignored since it is not supported by Unite.

Advanced parameters

Bleep each transmission:	This parameter was available in 942SI. The parameter is not available in Unite CM, instead the parameter can be set in advanced GUI under System 900 Advanced parameters.
Flow control XON/XOFF:	Not supported since there are some issues with the control characters. If the block check character becomes any of the two control characters XON or XOFF, the flow control fails, therefore flow control is no longer supported.

J.2 Ascom Line Protocol

J.2.1 Functionality

A line protocol message consists of the following records and separators:

<Addr/Message/Beepcode/PagFunc/NoOfTransm/Prio/Infopage>

All characters are writeable by hand using an ordinary terminal program such as hyper terminal etc. Not all records needs to be given, for instance <> is a valid message that delivers default message to default paging address.

J.2.2 Limitations

The following limitations apply:

PagFunc:	The Line protocol only supports call type 3 (plain paging) and 4 (alarm). All others are handled as plain paging.
NoOfTransm:	The Line protocol does not propagate number of transmissions but it must be valid if submitted. Number of transmissions can be set under System 900 and is then valid for all messages independent of the record value. Here it is also possible to determine number of transmissions based on the paging priority (advanced).
InfoPage:	The Line protocol does not propagate Infopage but it must be valid if submitted.

J.3 TAP Protocol

J.3.1 Functionality

- <ESC>PG1<CR>Default logon string
- First field of the data block is assumed to contain the paging address. The address is treated as a decimal address, valid digits is 0-9. Any leading spaces will be ignored.
- Field(s) after the first field is assumed to contain the paging text. If the datablock is containing more than 2 fields, fields 3,4,5.. will be concatenated to the paging text to be sent. (the separating <CR>:s will be treated as a part of the paging text. The paging text is set as 'Body' in the Unite paging. The 'Subject' will be empty.
- There is no restriction on how many blocks that can be sent during one logon session.

J.3.2 Limitations

The following limitations apply:

Using <US> or <ETB> as block terminators:	Not supported.
Maximum session timeout:	Not implemented, however an inactivity timeout will occur after 8 seconds when waiting for logon string and 4 seconds when waiting for block data after a <STX> has been received. After 3 successive timeouts, an automatic disconnect sequence will be initiated. These values can be changed through parameters.
Timeout between blocks:	There will be no timeout between blocks. After a logon has been received and after each paging block, the Serial Interface is put into sleep mode. Three actions can wake it up: A logoff request, a new logon request or a new paging block.
Messages longer than 128 characters:	Will be accepted but truncated.
Message sequences:	Not used by the Serial Interface.
Software flow control of the serialport:	Not supported.

Appendix K: Ascom Unite Application Manager

The Unite CM can either be used as a stand-alone module, or be used together with an Windows based Ascom Unite Application Manager (Unite AM). The Unite AM makes it possible to manage some features in Unite CM. When a feature is enabled in the Unite AM, the corresponding feature is disabled or hidden in the Unite CM. Refer to the Unite AM documentation for more information on how to manage the features.

Depending on the features enabled in the Unite AM, the following features might be affected in the Unite CM:

K.1 User Management

When users are managed from the Unite AM, the users will appear in the Unite CM. However, the users cannot be edited in Unite CM.

K.2 Duty Assignment

Duty Assignment is where locations, in for example a hospital, and definitions of conditions for Event Elements are set up.

When Unite Assign is enabled in the Unite AM, the Duty Assignment menu will be hidden in Unite CM. In this case, the work is done in the Unite AM.

K.3 Action Assignment

Events and actions and conditions for events, are configured here. The administration of access rights is also done in Action Assignment.

When the action assignment is managed from the Unite AM, the action assignment cannot be edited in the Unite CM. However, it is possible to view the settings in Unite CM.

K.4 Messaging Categories

When messages categories are managed from the Unite AM, the Messaging Categories menu in Unite CM will be hidden.

K.5 Groups

When Groups, Multicast groups and Broadcast groups are managed from the Unite AM, the groups will appear in the Unite CM. However, the groups cannot be edited in Unite CM.

Appendix L: Services in Unite CM

The Unite CM can distribute information to services enabled in the module itself, or distribute information to services enabled on another Unite module. Note that the services might be license dependent. Only use the services the Unite module have license for to avoid fault messages in the Unite module.

The destination to a service is written in the following format: IP address/service. For example: 127.0.0.1/DECT. Several features in Unite CM can have the same destination configured, but below is only one example described.

Service name	Description
ActivityLogger	Used to send activities in Unite CM to an Activity log. The destination to the service can for example be configured via System Activity Log settings. See 7.9 Logging on page 86.
Ascii	Used to interpret alarm and messages from different systems, receive messages via serial ports and enable access to external servers over HTTP. The destination to the service can for example be set via Advanced Event Handler configuration. See 4.11.3 Event Handler on page 53.
BasicAlarmHandler	Used to trigger the Basic Alarm Manager (BAM) that is a basic event handler making it possible to set up actions on incoming events. The destination to the service can for example be configured via Message Distribution settings. See 17.4 WLAN Message Distribution on page 138.
DECT	Used for communication via a DECT interface. The destination to the service can for example be configured via Device Management settings. See 6.2 Device Handling Configuration on page 75.
EventHandler	Used to trigger the Event Handler that is an advanced message handler making it possible to set up actions on incoming events. The destination to the service can for example be configured via Message Distribution settings. See 15.3.3 DECT Message Distribution on page 130.
FaultHandler	Used to send faults in Unite CM to a System log. The destination to the service can for example be configured via Log settings. See 7.9 Logging on page 86.
S900	Used for communication via an S900 paging interface. The destination to the service can for example be configured via Messaging Category settings. See 20.5 Add Messaging Category on page 161.
OAJ	Used to communicate with a Java Server with Java application installed. The destination to the service can for example be configured via Input Activity settings. See 4.8.4 Input Activity Distribution on page 43.
OAP	Used to communicate with other systems that require Open Access Protocol (OAP). The destination to the service can for example be configured via Message Distribution settings. See 17.4 WLAN Message Distribution on page 138.
Phonebook	Used to access the central phonebook.The destination to the service can for example be configured via Messaging Category settings. See 20.5 Add Messaging Category on page 161.

WLAN	Used for communication via a WLAN interface. The destination to the service can for example be configured via Device Management settings. See 6.2 Device Handling Configuration on page 75.
TAP	Used for sending messages via serial interface to other system that supports the TAP 1.8 protocol. The destination to the service can for example be configured via Messaging Category settings. See 20.5 Add Messaging Category on page 161.
ESPA	Used for sending messages via serial interface to other system that supports the ESPA 4.4.4. protocol. The destination to the service can for example be configured via Messaging Category settings. See 20.5 Add Messaging Category on page 161.
TextSigns	Used to provide information to text displays in teleCARE systems. The destination to the service can for example be configured via Messaging Category settings. See 20.5 Add Messaging Category on page 161.
mailgate	Used for sending messages to a mail address via external mail server. The destination to the service can for example be configured via Messaging Category settings. See 20.5 Add Messaging Category on page 161.
IO	Used for receiving input notifications and to set physical outputs. The destination to the service can for example be set via Advanced Event Handler configuration. See 4.11.3 Event Handler on page 53
ECG	Used to communicate with Cisco interface that is a gateway between the Unite messaging system and Cisco IP handsets. The destination to the service can for example be configured via Messaging Category settings. See 20.5 Add Messaging Category on page 161.

Appendix M: Multiple Event Handlers

This section describes the message flow when an external Event Handler (for example AMS or X-Gate) is connected to a Unite CM with Event Handler.

This solution can be used if you having an existing site and want to expand the site without having to upgrade the existing site.

See the example below for more information.

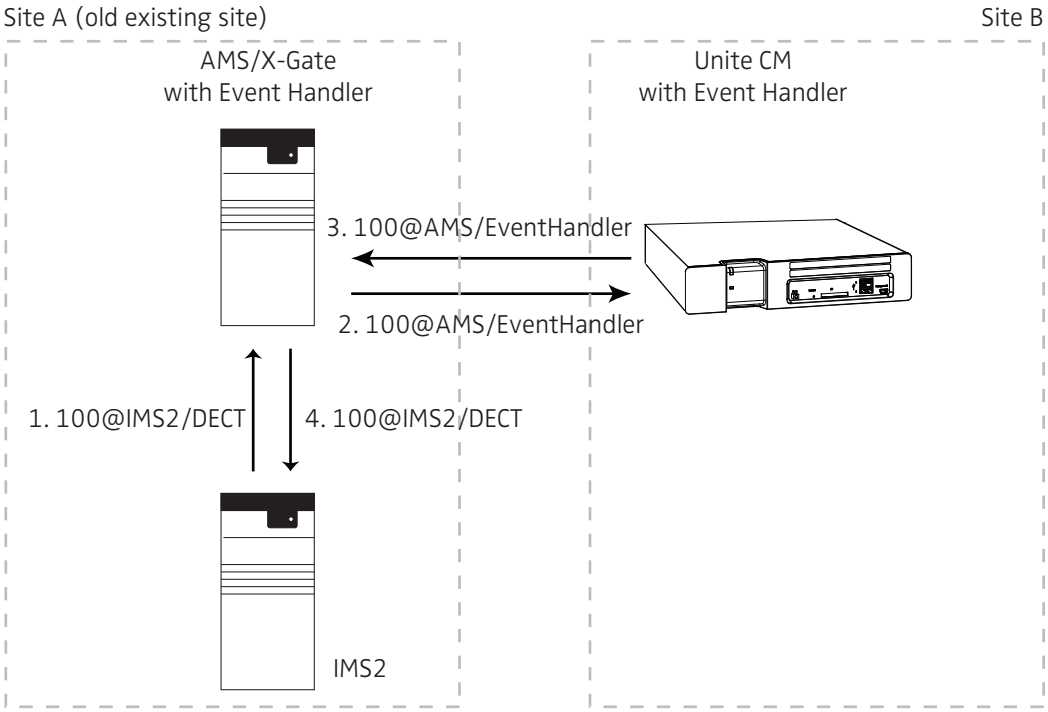


Figure 120. Communication between two Event Handlers.

In Figure 120 the Event Handlers on each site are configured to manage different kind of alarm messages.

For example, the Event Handler (AMS/X-Gate) is configured to manage alarm messages received from WLAN handsets, and the EventHandler (Unite CM) is configured to manage alarm messages received from DECT handsets.

1 The IMS2 forwards an alarm message, received from a DECT handset (Call ID: 100), to the Event Handler (AMS/X-Gate).

2 Since the alarm message is received from a DECT handset, the Event Handler (AMS/X-Gate) forwards the alarm message to the Event Handler (Unite CM). The Event Handler (Unite CM) accepts the alarm message received from the Event Handler (AMS/X-Gate). Note that the Call ID 100 is not configured as messaging user in Unite CM.

3 The Event Handler (Unite CM) can also send messages to a handset number, via Event Handler (AMS/X-Gate) without having the handset configured as messaging user in Unite CM.

4 The Event Handler (AMS/X-Gate) forwards the message to the IMS2, that in turn sends the message to the handset.

Conclusion: When sending messages between Event Handlers, the sender/receiver of the alarm message is not needed to be configured as messaging user in Unite CM.

Index

C

Central phonebook
CMG settings 95

D

DECT Interface 125
DECT interface
DECT phone systems
Alcatel OmniPCX Enterprise 125
IP-DECT
multiple systems 126
single system 126
Device Manager
devices
automatic detection of devices 77
device handling 75
status report for charges 75
status report for handsets 76
Digit manipulation..... 96

F

Firewall 208

L

LDAP Parameter Setup 93
Licence..... 89
Licences 1
Logging 86

M

Message Distribution..... 130, 138, 146

N

NetBIOS 18
Netpage..... 151
Network Settings..... 88

P

Passwords
password policy..... 17
set password complexity..... 17

R

Reboot..... 90

S

Security
NetBIOS..... 18
Service discovery 77
Set time 88
System 900 139

T

Time Settings 87

W

web messaging 151
WLAN Interface 137
WLAN System..... 137